NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Docum Secure Controls Framework (SCF) version 2025.2
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document: **Australia ISM June 2024**
Focal Document URL: https://www.cyber.gov.au/sites/default/files/2024-06/Information%20Security%20Manual%20%28June%202024%29.pdf
Published STRM URL: https://securecontrolsframework.com/content/strm/scf-strm-apac-australia-ism-june-2024.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	Essential 8 ML1	Essential 8 ML1	Essential 8 ML1	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
ISM-0027	N/A	System owners obtain authorisation to operate each system from its authorising officer based on the acceptance of the security risks associated with its operation.				Functional	intersects with	Authorize Systems, Applications & Services	GOV-15.4	Mechanisms exist to compel data and/or process owners to obtain authorization for the production use of each system, application and/or service under their control.	5	
ISM-0027	N/A	System owners obtain authorisation to operate each system from its authorising officer based on the acceptance of the security risks associated with its operation.				Functional	subset of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy assessment and authorization controls.	10	
ISM-0027	N/A	System owners obtain authorisation to operate each system from its authorising officer based on the acceptance of the security risks associated with its operation.				Functional	intersects with	Security Authorization	IAO-07	Mechanisms exist to ensure systems, projects and services are officially authorized prior to "go live" in a production environment.	5	
ISM-0039	N/A	A cyber security strategy is developed, implemented and maintained.				Functional	equal	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a strategic cybersecurity & data privacy-specific business plan and set of objectives to achieve that plan.	10	
ISM-0041	N/A	Systems have a system security plan that includes an overview of the system (covering the system's purpose, the system boundary and how the system is managed) as well as an annex that covers applicable controls from this document and any additional controls that have been identified and implemented.				Functional	equal	System Security & Privacy Plan (SSPP)	IAO-03	Mechanisms exist to generate System Security & Privacy Plans (SSPPs), or similar document repositories, to identify and maintain key architectural information on each critical system, application or service, as well as influence inputs, entities, systems, applications and processes, providing a historical record of the data and its origins.	10	
ISM-0042	N/A	System administration processes, and supporting system administration procedures, are developed, implemented and maintained.				Functional	equal	System Administrative Processes	AST-26	Mechanisms exist to develop, implement and govern system administration processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining systems, applications and services.	10	
ISM-0043	N/A	Systems have a cyber security incident response plan that covers the following: - guidelines on what constitutes a cyber security incident - the types of cyber security incidents likely to be encountered and the expected response to each type - how to report cyber security incidents, internally to an organisation and externally to relevant authorities - other parties which need to be informed in the event of a cyber security incident - the authority, or authorities, responsible for investigating and responding to cyber security incidents - the criteria by which an investigation of a cyber security incident would be requested from a law enforcement agency, the Australian Signals Directorate or other relevant authority - the steps necessary to ensure the integrity of evidence relating to a cyber security incident - system contingency measures or a reference to such details if they are located in a separate document.				Functional	equal	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	10	
ISM-0047	N/A	Organisational-level security documentation is approved by the Chief Information Security Officer while system-specific security documentation is approved by the system's authorising officer.				Functional	equal	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	10	
ISM-0072	N/A	Security requirements associated with the confidentiality, integrity and availability of data are documented in contractual arrangements with service providers and reviewed on a regular and ongoing basis to ensure they remain fit for purpose.				Functional	intersects with	Adequate Security for Sensitive / Regulated Data In Support of Contracts	IAO-03.2	Mechanisms exist to protect sensitive / regulated data that is collected, developed, received, transmitted, used or stored in support of the performance of a contract.	5	
ISM-0072	N/A	Security requirements associated with the confidentiality, integrity and availability of data are documented in contractual arrangements with service providers and reviewed on a regular and ongoing basis to ensure they remain fit for purpose.				Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
ISM-0078	N/A	Systems processing, storing or communicating AUSTEO or AGAO data remain at all times under the control of an Australian national working for or on behalf of the Australian Government.				Functional	subset of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
ISM-0100	N/A	Gateways undergo a security assessment by an IRAP assessor at least every 24 months.				Functional	intersects with	Independent Assessors	CPL-03.1	Mechanisms exist to utilize independent assessors to evaluate cybersecurity & data protection controls at planned intervals or when the system, service or project undergoes significant changes.	5	
ISM-0100	N/A	Gateways undergo a security assessment by an IRAP assessor at least every 24 months.				Functional	intersects with	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; and/or (11) Artificial Intelligence and Autonomous Technologies (AAT).	5	
ISM-0100	N/A	Gateways undergo a security assessment by an IRAP assessor at least every 24 months.				Functional	intersects with	Assessments	IAO-02	Mechanisms exist to formally assess the cybersecurity & data privacy controls in systems, applications and services through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5	
ISM-0100	N/A	Gateways undergo a security assessment by an IRAP assessor at least every 24 months.				Functional	intersects with	Third-Party Assessments	IAO-02.3	Mechanisms exist to accept and respond to the results of external assessments that are performed by impartial, external organizations.	5	
ISM-0109	N/A	Event logs from workstations are analysed in a timely manner to detect cyber security events.			ML3	Functional	subset of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	Essential Eight: ML3
ISM-0109	N/A	Event logs from workstations are analysed in a timely manner to detect cyber security events.			ML3	Functional	intersects with	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	Essential Eight: ML3
ISM-0109	N/A	Event logs from workstations are analysed in a timely manner to detect cyber security events.			ML3	Functional	intersects with	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	Essential Eight: ML3
ISM-0120	N/A	Cyber security personnel have access to sufficient data sources and tools to ensure that systems can be monitored for key indicators of compromise.				Functional	subset of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
ISM-0120	N/A	Cyber security personnel have access to sufficient data sources and tools to ensure that systems can be monitored for key indicators of compromise.				Functional	intersects with	Monitoring for Indicators of Compromise (IOC)	MON-11.3	Automated mechanisms exist to identify and alert on Indicators of Compromise (IoC).	5	
ISM-0123	N/A	Cyber security incidents are reported to the Chief Information Security Officer, or one of their delegates, as soon as possible after they occur or are discovered.		ML2	ML3	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	Essential Eight: ML2, ML3
ISM-0123	N/A	Cyber security incidents are reported to the Chief Information Security Officer, or one of their delegates, as soon as possible after they occur or are discovered.				Functional	intersects with	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.	5	
ISM-0125	N/A	A cyber security incident register is developed, implemented and maintained.				Functional	equal	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity & data privacy incidents to internal stakeholders all the way through the resolution of the incident.	10	
ISM-0133	N/A	When a data spill occurs, data owners are advised and access to the data is restricted.				Functional	intersects with	Sensitive / Regulated Data Spill Response	IRO-12	Mechanisms exist to respond to sensitive /regulated data spills.	5	
ISM-0133	N/A	When a data spill occurs, data owners are advised and access to the data is restricted.				Functional	intersects with	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	5	
ISM-0133	N/A	When a data spill occurs, data owners are advised and access to the data is restricted.				Functional	intersects with	Post-Sensitive / Regulated Data Spill Operations	IRO-12.3	Mechanisms exist to ensure that organizational personnel impacted by sensitive /regulated data spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.	5	
ISM-0133	N/A	When a data spill occurs, data owners are advised and access to the data is restricted.				Functional	intersects with	Sensitive / Regulated Data Exposure to Unauthorized Personnel	IRO-12.4	Mechanisms exist to address security safeguards for personnel exposed to sensitive /regulated data that is not within their assigned access authorizations.	5	
ISM-0137	N/A	Legal advice is sought before allowing intrusion activity to continue on a system for the purpose of collecting further data or evidence.				Functional	subset of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	10	
ISM-0137	N/A	Legal advice is sought before allowing intrusion activity to continue on a system for the purpose of collecting further data or evidence.				Functional	intersects with	Chain of Custody & Forensics	IRO-08	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	5	
ISM-0137	N/A	Legal advice is sought before allowing intrusion activity to continue on a system for the purpose of collecting further data or evidence.				Functional	intersects with	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity & data privacy incidents to internal stakeholders all the way through the resolution of the incident.	5	
ISM-0137	N/A	Legal advice is sought before allowing intrusion activity to continue on a system for the purpose of collecting further data or evidence.				Functional	intersects with	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.	5	
ISM-0138	N/A	The integrity of evidence gathered during an investigation is maintained by investigators: - recording all of their actions - maintaining a proper chain of custody - following all instructions provided by relevant law enforcement agencies.				Functional	equal	Chain of Custody & Forensics	IRO-08	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	Essential 8 ML1	Essential 8 ML1	Essential 8 ML1	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
ISM-0140	N/A	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.		ML2	ML3	Functional	equal	Regulatory & Law Enforcement Contacts	IRO-14	Mechanisms exist to maintain incident response contacts with applicable regulatory and law enforcement agencies.	10	Essential Eight: ML2, ML3
ISM-0141	N/A	The requirement for service providers to report cyber security incidents to a designated point of contact as soon as possible after they occur or are discovered is documented in contractual arrangements with service providers.				Functional	equal	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
ISM-0142	N/A	The compromise or suspected compromise of cryptographic equipment or associated keying material is reported to the Chief Information Security Officer, or one of their delegates, as soon as possible after it occurs.				Functional	subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
ISM-0161	N/A	IT equipment and media are secured when not in use				Functional	intersects with	Security of Assets & Media	AST-05	Mechanisms exist to maintain strict control over the internal or external distribution of any kind of sensitive/regulated media.	5	
ISM-0161	N/A	IT equipment and media are secured when not in use.				Functional	intersects with	Unattended End-User Equipment	AST-06	Mechanisms exist to implement enhanced protection measures for unattended systems to protect against tampering and unauthorized access.	5	
ISM-0164	N/A	Unauthorised people are prevented from observing systems, in particular workstation displays and keyboards, within facilities.				Functional	intersects with	Restrict Unescorted Access	PES-06.3	Physical access control mechanisms exist to restrict unescorted access to facilities to personnel with required security clearances, formal access authorizations and validate the need for access.	5	
ISM-0164	N/A	Unauthorised people are prevented from observing systems, in particular workstation displays and keyboards, within facilities.				Functional	intersects with	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	5	
ISM-0164	N/A	Unauthorised people are prevented from observing systems, in particular workstation displays and keyboards, within facilities.				Functional	intersects with	Working in Secure Areas	PES-04.1	Physical security mechanisms exist to allow only authorized personnel access to secure areas.	5	
ISM-0181	N/A	Cabling infrastructure is installed in accordance with relevant Australian Standards, as directed by the Australian Communications and Media Authority.				Functional	subset of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
ISM-0187	N/A	SECRET cables, when bundled together or run in conduit, are run exclusively in their own individual cable bundle or conduit.				Functional	subset of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
ISM-0194	N/A	In shared facilities, a visible smear of conduit glue is used to seal all plastic conduit joints and TOP SECRET conduits connected by threaded lock nuts.				Functional	subset of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
ISM-0195	N/A	In shared facilities, uniquely identifiable SCEC-approved tamper-evident seals are used to seal all removable covers on TOP SECRET cable reticulation systems.				Functional	subset of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
ISM-0198	N/A	When penetrating a TOP SECRET audio secure room, the Australian Security Intelligence Organisation is consulted and all directions provided are complied with.				Functional	subset of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
ISM-0201	N/A	Labels for TOP SECRET conduits are a minimum size of 2.5 cm x 1 cm, attached at five-metre intervals and marked as 'TS RUN'.				Functional	intersects with	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
ISM-0201	N/A	Labels for TOP SECRET conduits are a minimum size of 2.5 cm x 1 cm, attached at five-metre intervals and marked as 'TS RUN'.				Functional	intersects with	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
ISM-0206	N/A	Cable labelling processes, and supporting cable labelling procedures, are developed, implemented and maintained.				Functional	subset of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
ISM-0208	N/A	A cable register contains the following for each cable: - cable identifier - cable colour - sensitivity/classification - source - destination - location - seal numbers (if applicable).				Functional	subset of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
ISM-0211	N/A	A cable register is developed, implemented, maintained and verified on a regular basis.				Functional	subset of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
ISM-0213	N/A	SECRET and TOP SECRET cables are terminated on their own individual patch panels.				Functional	subset of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
ISM-0216	N/A	TOP SECRET patch panels are installed in individual TOP SECRET cabinets.				Functional	subset of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
ISM-0217	N/A	Where spatial constraints demand non-TOP SECRET patch panels be installed in the same cabinet as a TOP SECRET patch panel: - a physical barrier in the cabinet is provided to separate patch panels - only personnel holding a Positive Vetting security clearance have access to the cabinet - approval from the TOP SECRET system's authorising officer is obtained prior to installation.				Functional	subset of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
ISM-0218	N/A	If TOP SECRET fibre-optic fly leads exceeding five metres in length are used to connect wall outlet boxes to IT equipment, they are run in a protective and easily inspected pathway that is clearly labelled at the IT equipment end with the wall outlet box's identifier.				Functional	subset of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
ISM-0225	N/A	Unauthorised RF and IR devices are not brought into SECRET and TOP SECRET areas.				Functional	subset of	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	10	
ISM-0229	N/A	Personnel are advised of the permitted sensitivity or classification of information that can be discussed over internal and external telephone systems				Functional	intersects with	Use of Communications Technology	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously.	5	
ISM-0229	N/A	Personnel are advised of the permitted sensitivity or classification of information that can be discussed over both internal and external telephone systems.				Functional	intersects with	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
ISM-0230	N/A	Personnel are advised of security risks posed by non-secure telephone systems in areas where sensitive or classified conversations can occur.				Functional	intersects with	Use of Communications Technology	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously.	5	
ISM-0230	N/A	Personnel are advised of security risks posed by non-secure telephone systems in areas where sensitive or classified conversations can occur.				Functional	intersects with	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
ISM-0231	N/A	When using cryptographic equipment to permit different levels of conversation for different kinds of connections, telephone systems give a visual indication of what kind of connection has been made.				Functional	intersects with	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
ISM-0231	N/A	When using cryptographic equipment to permit different levels of conversation for different kinds of connections, telephone systems give a visual indication of what kind of connection has been made.				Functional	intersects with	Collaborative Computing Devices	END-14	Mechanisms exist to unplug or prohibit the remote activation of collaborative computing devices with the following exceptions: (1) Networked whiteboards; (2) Video teleconference cameras; and (3) Teleconference microphones.	5	
ISM-0232	N/A	Telephone systems used for sensitive or classified conversations encrypt all traffic that passes over external systems.				Functional	subset of	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	10	
ISM-0233	N/A	Cordless telephone handsets and headsets are not used for sensitive or classified conversations unless all communications are encrypted.				Functional	intersects with	Bluetooth & Wireless Devices	AST-14.1	Mechanisms exist to prevent the usage of Bluetooth and wireless devices (e.g., Near Field Communications (NFC)) in sensitive areas or unless used in a Radio Frequency (RF)-screened building.	5	
ISM-0233	N/A	Cordless telephone handsets and headsets are not used for sensitive or classified conversations unless all communications are encrypted.				Functional	intersects with	Use of Communications Technology	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously.	5	
ISM-0235	N/A	Speakerphones are not used on telephone systems in TOP SECRET areas unless the telephone system is located in an audio secure room, the room is audio secure during conversations and only personnel involved in conversations are present in the room.				Functional	subset of	Use of Communications Technology	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously.	10	
ISM-0236	N/A	Off-hook audio protection features are used on telephone systems in areas where background conversations may exceed the sensitivity or classification that the telephone system is authorised for communicating.				Functional	subset of	Use of Communications Technology	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously.	10	
ISM-0240	N/A	Paging, Multimedia Message Service, Short Message Service and messaging apps are not used to communicate sensitive or classified data.				Functional	intersects with	Use of Communications Technology	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously.	5	
ISM-0240	N/A	Paging, Multimedia Message Service, Short Message Service and messaging apps are not used to communicate sensitive or classified data.				Functional	intersects with	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
ISM-0241	N/A	When sending fax messages, the fax message is encrypted to an appropriate level to be communicated over unsecured telecommunications infrastructure.				Functional	intersects with	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
ISM-0241	N/A	When sending fax messages, the fax message is encrypted to an appropriate level to be communicated over unsecured telecommunications infrastructure.				Functional	intersects with	Use of Communications Technology	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously.	5	
ISM-0245	N/A	A direct connection from an MFD to a digital telephone system is not enabled unless the digital telephone system is authorised to operate at the same sensitivity or classification as the network to which the MFD is connected.				Functional	subset of	Multi-Function Devices (MFD)	AST-23	Mechanisms exist to securely configure Multi-Function Devices (MFD) according to industry-recognized secure practices for the type of device.	10	
ISM-0246	N/A	When an emanation security threat assessment is required, it is sought as early as possible in a system's life cycle.				Functional	subset of	Information Leakage Due To Electromagnetic Signals Emanations	PES-13	Facility security mechanisms exist to protect the system from information leakage due to electromagnetic signals emanations.	10	
ISM-0248	N/A	System owners deploying OFFICIAL: Sensitive or PROTECTED systems with radio frequency transmitters (including any wireless capabilities) that will be located within 20 meters of SECRET or TOP SECRET systems contact ASD for an emanation security threat assessment.				Functional	subset of	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	10	
ISM-0249	N/A	System owners deploying SECRET or TOP SECRET systems in mobile platforms, or as a deployable capability, contact ASD for an emanation security threat assessment.				Functional	subset of	Information Leakage Due To Electromagnetic Signals Emanations	PES-13	Facility security mechanisms exist to protect the system from information leakage due to electromagnetic signals emanations.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	Essential 8 ML1	Essential 8 ML1	Essential 8 ML1	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
ISM-0250	N/A	IT equipment meets industry and government standards relating to electromagnetic interference/electromagnetic compatibility.				Functional	subset of	Information Leakage Due To Electromagnetic Signals Emanations	PES-13	Facility security mechanisms exist to protect the system from information leakage due to electromagnetic signals emanations.	10	
ISM-0252	N/A	Cyber security awareness training is undertaken annually by all personnel and covers: - the purpose of the cyber security awareness training - security appointments and contacts - authorised use of systems and their resources - protection of systems and their resources - reporting of cyber security incidents and suspected compromises of systems and their resources.				Functional	subset of	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
ISM-0252	N/A	Cyber security awareness training is undertaken annually by all personnel and covers: - the purpose of the cyber security awareness training - security appointments and contacts - authorised use of systems and their resources - protection of systems and their resources - reporting of cyber security incidents and suspected compromises of systems and their resources.				Functional	intersects with	Cybersecurity & Data Privacy Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	
ISM-0258	N/A	A web usage policy is developed, implemented and maintained.				Functional	subset of	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	10	
ISM-0260	N/A	All web access, including that by internal servers, is conducted through web proxies.				Functional	subset of	Route Internal Traffic to Proxy Servers	NET-18.1	Mechanisms exist to route internal communications traffic to external networks through organization-approved proxy servers at managed interfaces.	10	
ISM-0261	N/A	The following details are centrally logged for websites accessed via web proxies: - web address - date and time - user - amount of data uploaded and downloaded - internal and external IP addresses.				Functional	equal	Proxy Logging	MON-01.9	Mechanisms exist to log all Internet-bound requests, in order to identify prohibited activities and assist incident handlers with identifying potentially compromised systems.	10	
ISM-0263	N/A	TLS traffic communicated through gateways is decrypted and inspected.				Functional	equal	Visibility of Encrypted Communications	NET-18.2	Mechanisms exist to configure the proxy to make encrypted communications traffic visible to monitoring tools and mechanisms.	10	
ISM-0264	N/A	An email usage policy is developed, implemented and maintained.				Functional	intersects with	Use of Communications Technology	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously.	5	
ISM-0264	N/A	An email usage policy is developed, implemented and maintained.				Functional	intersects with	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
ISM-0267	N/A	Access to non-approved webmail services is blocked.				Functional	intersects with	Use of Communications Technology	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously.	5	
ISM-0267	N/A	Access to non-approved webmail services is blocked.				Functional	intersects with	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
ISM-0267	N/A	Access to non-approved webmail services is blocked.				Functional	intersects with	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
ISM-0269	N/A	Emails containing Australian Eyes Only, Australian Government Access Only or Releasable To data are not sent to email distribution lists unless the nationality of all members of email distribution lists can be confirmed.				Functional	subset of	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	10	
ISM-0270	N/A	Protective markings are applied to emails and reflect the highest sensitivity or classification of the subject, body and attachments.				Functional	intersects with	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
ISM-0270	N/A	Protective markings are applied to emails and reflect the highest sensitivity or classification of the subject, body and attachments.				Functional	intersects with	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
ISM-0270	N/A	Protective markings are applied to emails and reflect the highest sensitivity or classification of the subject, body and attachments.				Functional	intersects with	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
ISM-0271	N/A	Protective marking tools do not automatically insert protective markings into emails.				Functional	intersects with	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
ISM-0271	N/A	Protective marking tools do not automatically insert protective markings into emails.				Functional	intersects with	Automated Marking	DCH-04.1	Automated mechanisms exist to mark physical media and digital files to indicate the distribution limitations, handling requirements and applicable security markings (if any) of the information to aid Data Loss Prevention (DLP) technologies.	5	
ISM-0271	N/A	Protective marking tools do not automatically insert protective markings into emails.				Functional	intersects with	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
ISM-0272	N/A	Protective marking tools do not allow users to select protective markings that a system has not been authorised to process, store or communicate.				Functional	intersects with	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
ISM-0272	N/A	Protective marking tools do not allow users to select protective markings that a system has not been authorised to process, store or communicate.				Functional	intersects with	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
ISM-0272	N/A	Protective marking tools do not allow users to select protective markings that a system has not been authorised to process, store or communicate.				Functional	intersects with	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
ISM-0280	N/A	If procuring an evaluated product, a product that has completed a PP-based evaluation, including against all applicable PP modules, is selected in preference to one that has completed an EAL-based evaluation.				Functional	subset of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy assessment and authorization controls.	10	
ISM-0285	N/A	Evaluated products are delivered in a manner consistent with any delivery procedures defined in associated evaluation documentation.				Functional	subset of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
ISM-0286	N/A	When procuring high assurance IT equipment, ASD is contacted for any equipment-specific delivery procedures.				Functional	subset of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
ISM-0289	N/A	Evaluated products are installed, configured, administered and operated in an evaluated configuration and in accordance with vendor guidance.				Functional	subset of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
ISM-0290	N/A	High assurance IT equipment is installed, configured, administered and operated in an evaluated configuration and in accordance with ASD guidance.				Functional	subset of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
ISM-0293	N/A	IT equipment is classified based on the highest sensitivity or classification of data that it is approved for processing, storing or communicating.				Functional	intersects with	Security of Assets & Media	AST-05	Mechanisms exist to maintain strict control over the internal or external distribution of any kind of sensitive/regulated media.	5	
ISM-0293	N/A	IT equipment is classified based on the highest sensitivity or classification of data that it is approved for processing, storing or communicating.				Functional	intersects with	Security Authorization	IAO-07	Mechanisms exist to ensure systems, projects and services are officially authorized prior to "go live" in a production environment.	5	
ISM-0294	N/A	IT equipment, with the exception of high assurance IT equipment, is labelled with protective markings reflecting its sensitivity or classification.				Functional	intersects with	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
ISM-0294	N/A	IT equipment, with the exception of high assurance IT equipment, is labelled with protective markings reflecting its sensitivity or classification.				Functional	intersects with	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
ISM-0296	N/A	ASD's approval is sought before applying labels to external surfaces of high assurance IT equipment.				Functional	intersects with	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
ISM-0296	N/A	ASD's approval is sought before applying labels to external surfaces of high assurance IT equipment.				Functional	intersects with	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
ISM-0298	N/A	A centralised and managed approach that maintains the integrity of patches or updates, and confirms that they have been applied successfully, is used to patch or update applications, operating systems, drivers and firmware.				Functional	equal	Centralized Management of Flaw Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	10	
ISM-0300	N/A	Patches, updates or other vendor mitigations for vulnerabilities in high assurance IT equipment are applied only when approved by ASD, and in doing so, using methods and timeframes prescribed by ASD.				Functional	subset of	Centralized Management of Flaw Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	10	
ISM-0304	N/A	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.			ML3	Functional	subset of	Unsupported Systems	TDA-17	Mechanisms exist to prevent unsupported systems by: (1) Replacing systems 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 system components required to satisfy mission/business needs.	10	Essential Eight: ML3
ISM-0305	N/A	Maintenance and repairs of IT equipment is carried out on site by an appropriately cleared technician.				Functional	subset of	Maintenance Operations	MNT-01	Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise.	10	
ISM-0305	N/A	Maintenance and repairs of IT equipment is carried out on site by an appropriately cleared technician.				Functional	intersects with	Authorized Maintenance Personnel	MNT-06	Mechanisms exist to maintain a current list of authorized maintenance organizations or personnel.	5	
ISM-0305	N/A	Maintenance and repairs of IT equipment is carried out on site by an appropriately cleared technician.				Functional	intersects with	Field Maintenance	MNT-08	Mechanisms exist to securely conduct field maintenance on geographically deployed assets.	5	
ISM-0306	N/A	If an appropriately cleared technician is not used to undertake maintenance or repairs of IT equipment, the technician is escorted by someone who: - is appropriately cleared and briefed - takes due care to ensure that data is not disclosed - takes all responsible measures to ensure the integrity of the IT equipment - has the authority to direct the technician - is sufficiently familiar with the IT equipment to understand the work being performed.				Functional	subset of	Maintenance Personnel Without Appropriate Access	MNT-06.1	Mechanisms exist to ensure the risks associated with maintenance personnel who do not have appropriate access authorizations, clearances or formal access approvals are appropriately mitigated.	10	
ISM-0307	N/A	If an appropriately cleared technician is not used to undertake maintenance or repairs of IT equipment, the IT equipment and associated media is sanitised before maintenance or repair work is undertaken.				Functional	subset of	Authorized Maintenance Personnel	MNT-06	Mechanisms exist to maintain a current list of authorized maintenance organizations or personnel.	10	
ISM-0310	N/A	IT equipment maintained or repaired off site is done so at facilities approved for handling the sensitivity or classification of the IT equipment.				Functional	intersects with	Off-Site Maintenance	MNT-09	Mechanisms exist to ensure off-site maintenance activities are conducted securely and the asset(s) undergoing maintenance actions are secured during physical transfer and storage while off-site.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	Essential 8 ML1	Essential 8 ML1	Essential 8 ML1	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
ISM-0311	N/A	IT equipment containing media is sanitised by removing the media from the IT equipment or by sanitising the media in situ.				Functional	intersects with	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
ISM-0311	N/A	IT equipment containing media is sanitised by removing the media from the IT equipment or by sanitising the media in situ.				Functional	intersects with	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
ISM-0311	N/A	IT equipment containing media is sanitised by removing the media from the IT equipment or by sanitising the media in situ.				Functional	intersects with	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
ISM-0311	N/A	IT equipment containing media is sanitised by removing the media from the IT equipment or by sanitising the media in situ.				Functional	intersects with	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
ISM-0311	N/A	IT equipment containing media is sanitised by removing the media from the IT equipment or by sanitising the media in situ.				Functional	intersects with	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
ISM-0311	N/A	IT equipment containing media is sanitised by removing the media from the IT equipment or by sanitising the media in situ.				Functional	intersects with	Information Disposal	DCH-21	Mechanisms exist to securely dispose of, destroy or erase information.	5	
ISM-0312	N/A	IT equipment, including associated media, that is located overseas and has processed, stored or communicated AUSTEO or AGAO data that cannot be sanitised in situ, is returned to Australia for destruction.				Functional	intersects with	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
ISM-0312	N/A	IT equipment, including associated media, that is located overseas and has processed, stored or communicated AUSTEO or AGAO data that cannot be sanitised in situ, is returned to Australia for destruction.				Functional	intersects with	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
ISM-0313	N/A	IT equipment sanitisation processes, and supporting IT equipment sanitisation procedures, are developed, implemented and maintained.				Functional	equal	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	10	
ISM-0315	N/A	High assurance IT equipment is destroyed prior to its disposal.				Functional	intersects with	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
ISM-0315	N/A	High assurance IT equipment is destroyed prior to its disposal.				Functional	intersects with	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
ISM-0316	N/A	Following sanitisation, destruction or declassification, a formal administrative decision is made to release IT equipment, or its waste, into the public domain.				Functional	subset of	System Media Sanitization Documentation	DCH-09.1	Mechanisms exist to supervise, track, document and verify system media sanitization and disposal actions.	10	
ISM-0317	N/A	At least three pages of random text with no blank areas are printed on each colour printer cartridge or MFD print drum.				Functional	subset of	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	10	
ISM-0318	N/A	When unable to sanitise printer cartridges or MFD print drums, they are destroyed as per electrostatic memory devices.				Functional	subset of	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	10	
ISM-0321	N/A	When disposing of IT equipment that has been designed or modified to meet emanation security standards, ASD is contacted for requirements relating to its disposal.				Functional	subset of	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	10	
ISM-0323	N/A	Media is classified to the highest sensitivity or classification of data it stores, unless the media has been classified to a higher sensitivity or classification.				Functional	intersects with	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
ISM-0323	N/A	Media is classified to the highest sensitivity or classification of data it stores, unless the media has been classified to a higher sensitivity or classification.				Functional	intersects with	Highest Classification Level	DCH-02.1	Mechanisms exist to ensure that systems, applications and services are classified according to the highest level of data sensitivity that is stored, transmitted and/or processed.	5	
ISM-0325	N/A	Any media connected to a system with a higher sensitivity or classification than the media is reclassified to the higher sensitivity or classification, unless the media is read-only or the system has a mechanism through which read-only access can be ensured.				Functional	intersects with	Highest Classification Level	DCH-02.1	Mechanisms exist to ensure that systems, applications and services are classified according to the highest level of data sensitivity that is stored, transmitted and/or processed.	5	
ISM-0325	N/A	Any media connected to a system with a higher sensitivity or classification than the media is reclassified to the higher sensitivity or classification, unless the media is read-only or the system has a mechanism through which read-only access can be ensured.				Functional	intersects with	Attribute Reassignment	DCH-05.9	Mechanisms exist to reclassify data as required, due to changing business/technical requirements.	5	
ISM-0325	N/A	Any media connected to a system with a higher sensitivity or classification than the media is reclassified to the higher sensitivity or classification, unless the media is read-only or the system has a mechanism through which read-only access can be ensured.				Functional	intersects with	Data Reclassification	DCH-11	Mechanisms exist to reclassify data, including associated systems, applications and services, commensurate with the security category and/or classification level of the information.	5	
ISM-0330	N/A	Before reclassifying media to a lower sensitivity or classification, the media is sanitised or destroyed, and a formal administrative decision is made to reclassify it.				Functional	intersects with	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
ISM-0330	N/A	Before reclassifying media to a lower sensitivity or classification, the media is sanitised or destroyed, and a formal administrative decision is made to reclassify it.				Functional	intersects with	Data Reclassification	DCH-11	Mechanisms exist to reclassify data, including associated systems, applications and services, commensurate with the security category and/or classification level of the information.	5	
ISM-0332	N/A	Media, with the exception of internally mounted fixed media within IT equipment, is labelled with protective markings reflecting its sensitivity or classification.				Functional	equal	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	10	
ISM-0336	N/A	A networked IT equipment register is developed, implemented, maintained and verified on a regular basis.				Functional	intersects with	Asset Inventories	AST-02	Mechanisms exist to maintain a current list of approved technologies (hardware and software).	5	
ISM-0336	N/A	A networked IT equipment register is developed, implemented, maintained and verified on a regular basis.				Functional	intersects with	Sensitive Data Inventories	DCH-06.2	Mechanisms exist to maintain inventory logs of all sensitive media and conduct sensitive media inventories at least annually.	5	
ISM-0337	N/A	Media is only used with systems that are authorised to process, store or communicate its sensitivity or classification.				Functional	subset of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
ISM-0341	N/A	Automatic execution features for removable media are disabled.				Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
ISM-0341	N/A	Automatic execution features for removable media are disabled.				Functional	intersects with	Media Use	DCH-10	Mechanisms exist to restrict the use of types of digital media on systems or system components.	5	
ISM-0343	N/A	If there is no business requirement for writing to removable media and devices, such functionality is disabled via the use of device access control software or by disabling external communication interfaces.				Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
ISM-0343	N/A	If there is no business requirement for writing to removable media and devices, such functionality is disabled via the use of device access control software or by disabling external communication interfaces.				Functional	intersects with	Media Use	DCH-10	Mechanisms exist to restrict the use of types of digital media on systems or system components.	5	
ISM-0343	N/A	If there is no business requirement for writing to removable media and devices, such functionality is disabled via the use of device access control software or by disabling external communication interfaces.				Functional	intersects with	Limitations on Use	DCH-10.1	Mechanisms exist to restrict the use and distribution of sensitive / regulated data.	5	
ISM-0345	N/A	External communication interfaces that allow DMA are disabled.				Functional	subset of	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	10	
ISM-0347	N/A	When transferring data manually between two systems belonging to different security domains, write-once media is used unless the destination system has a mechanism through which read-only access can be ensured.				Functional	subset of	Ad-Hoc Transfers	DCH-17	Mechanisms exist to secure ad-hoc exchanges of large digital files with internal or external parties.	10	
ISM-0348	N/A	Media sanitisation processes, and supporting media sanitisation procedures, are developed, implemented and maintained.				Functional	equal	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	10	
ISM-0350	N/A	The following media types are destroyed prior to their disposal: - microfiche and microfilm - optical discs - programmable read-only memory - read-only memory - other types of media that cannot be sanitised.				Functional	equal	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	10	
ISM-0351	N/A	Volatile media is sanitised by removing its power for at least 10 minutes.				Functional	subset of	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	10	
ISM-0352	N/A	SECRET and TOP SECRET volatile media is sanitised by overwriting it at least once in its entirety with a random pattern followed by a read back for verification.				Functional	subset of	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	10	
ISM-0354	N/A	Non-volatile magnetic media is sanitised by overwriting it at least once (or three times if pre-2001 or under 15 GB) in its entirety with a random pattern followed by a read back for verification.				Functional	subset of	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	10	
ISM-0356	N/A	Following sanitisation, SECRET and TOP SECRET non-volatile magnetic media retains its classification.				Functional	intersects with	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
ISM-0356	N/A	Following sanitisation, SECRET and TOP SECRET non-volatile magnetic media retains its classification.				Functional	intersects with	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
ISM-0357	N/A	Non-volatile EPROM media is sanitised by applying three times the manufacturer's specified ultraviolet erasure time and then overwriting it at least once in its entirety with a random pattern followed by a read back for verification.				Functional	subset of	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	Essential 8 ML1	Essential 8 ML1	Essential 8 ML1	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
ISM-0358	N/A	Following sanitisation, SECRET and TOP SECRET non-volatile EPROM and EEPROM media retains its classification.				Functional	intersects with	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
ISM-0358	N/A	Following sanitisation, SECRET and TOP SECRET non-volatile EPROM and EEPROM media retains its classification.				Functional	intersects with	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
ISM-0359	N/A	Non-volatile flash memory media is sanitised by overwriting it at least twice in its entirety with a random pattern followed by a read back for verification.				Functional	subset of	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	10	
ISM-0360	N/A	Following sanitisation, SECRET and TOP SECRET non-volatile flash memory media retains its classification.				Functional	intersects with	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
ISM-0360	N/A	Following sanitisation, SECRET and TOP SECRET non-volatile flash memory media retains its classification.				Functional	intersects with	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
ISM-0361	N/A	Magnetic media is destroyed using a degausser with a suitable magnetic field strength and magnetic orientation.				Functional	subset of	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	10	
ISM-0362	N/A	Product-specific directions provided by degausser manufacturers are followed.				Functional	subset of	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	10	
ISM-0363	N/A	Media destruction processes, and supporting media destruction procedures, are developed, implemented and maintained.				Functional	intersects with	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
ISM-0363	N/A	Media destruction processes, and supporting media destruction procedures, are developed, implemented and maintained.				Functional	intersects with	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
ISM-0363	N/A	Media destruction processes, and supporting media destruction procedures, are developed, implemented and maintained.				Functional	intersects with	System Media Sanitization Documentation	DCH-09.1	Mechanisms exist to supervise, track, document and verify system media sanitization and disposal actions.	5	
ISM-0368	N/A	Media destroyed using a hammer mill, disintegrator, grinder/sander or by cutting results in media waste particles no larger than 9 mm.				Functional	subset of	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	10	
ISM-0370	N/A	The destruction of media is performed under the supervision of at least one cleared person.				Functional	intersects with	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
ISM-0370	N/A	The destruction of media is performed under the supervision of at least one cleared person.				Functional	intersects with	System Media Sanitization Documentation	DCH-09.1	Mechanisms exist to supervise, track, document and verify system media sanitization and disposal actions.	5	
ISM-0371	N/A	Personnel supervising the destruction of media supervise its handling to the point of destruction and ensure that the destruction is completed successfully.				Functional	subset of	System Media Sanitization Documentation	DCH-09.1	Mechanisms exist to supervise, track, document and verify system media sanitization and disposal actions.	10	
ISM-0372	N/A	The destruction of media storing accountable material is performed under the supervision of at least two cleared personnel.				Functional	intersects with	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
ISM-0372	N/A	The destruction of media storing accountable material is performed under the supervision of at least two cleared personnel.				Functional	intersects with	System Media Sanitization Documentation	DCH-09.1	Mechanisms exist to supervise, track, document and verify system media sanitization and disposal actions.	5	
ISM-0373	N/A	Personnel supervising the destruction of media storing accountable material supervise its handling to the point of destruction, ensure that the destruction is completed successfully and sign a destruction certificate afterwards.				Functional	subset of	System Media Sanitization Documentation	DCH-09.1	Mechanisms exist to supervise, track, document and verify system media sanitization and disposal actions.	10	
ISM-0374	N/A	Media disposal processes, and supporting media disposal procedures, are developed, implemented and maintained.				Functional	subset of	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	10	
ISM-0375	N/A	Following sanitisation, destruction or declassification, a formal administrative decision is made to release media, or its waste, into the public domain.				Functional	subset of	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	10	
ISM-0378	N/A	Labels and markings indicating the owner, sensitivity, classification or any other marking that can associate media with its prior use are removed prior to its disposal.				Functional	intersects with	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
ISM-0378	N/A	Labels and markings indicating the owner, sensitivity, classification or any other marking that can associate media with its prior use are removed prior to its disposal.				Functional	intersects with	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
ISM-0380	N/A	Unneeded accounts, components, services and functionality of operating systems are disabled or removed.				Functional	subset of	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	10	
ISM-0382	N/A	Unprivileged users do not have the ability to uninstall or disable approved software.				Functional	intersects with	User-Installed Software	CFG-05	Mechanisms exist to restrict the ability of non-privileged users to install unauthorized software.	5	
ISM-0382	N/A	Unprivileged users do not have the ability to uninstall or disable approved software.				Functional	intersects with	Restrict Roles Permitted To Install Software	CFG-05.2	Mechanisms exist to configure systems to prevent the installation of software, unless the action is performed by a privileged user or service.	5	
ISM-0383	N/A	Default accounts or credentials for operating systems, including for any pre-configured accounts, are changed.				Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
ISM-0383	N/A	Default accounts or credentials for operating systems, including for any pre-configured accounts, are changed.				Functional	intersects with	Secure Settings By Default	TDA-09.6	Mechanisms exist to implement secure configuration settings by default to reduce the likelihood of software being deployed with weak security settings that would put the asset at a greater risk of compromise.	5	
ISM-0385	N/A	Servers maintain effective functional separation with other servers allowing them to operate independently.				Functional	subset of	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	10	
ISM-0393	N/A	Databases and their contents are classified based on the sensitivity or classification of data that they contain.				Functional	intersects with	Database Administrative Processes	AST-28	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	5	
ISM-0393	N/A	Databases and their contents are classified based on the sensitivity or classification of data that they contain.				Functional	intersects with	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
ISM-0400	N/A	Development, testing and production environments are segregated.				Functional	intersects with	Secure Development Environments	TDA-07	Mechanisms exist to maintain a segmented development network to ensure a secure development environment.	5	
ISM-0400	N/A	Development, testing and production environments are segregated.				Functional	intersects with	Separation of Development, Testing and Operational Environments	TDA-08	Mechanisms exist to manage separate development, testing and operational environments to reduce the risks of unauthorized access or changes to the operational environment and to ensure no impact to production systems.	5	
ISM-0401	N/A	Secure-by-design and secure-by-default principles, use of memory-safe programming languages where possible, and secure programming practices are used as part of application development.				Functional	subset of	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	10	
ISM-0402	N/A	Applications are comprehensively tested for vulnerabilities, using static application security testing and dynamic application security testing, prior to their initial release and any subsequent releases.				Functional	intersects with	Cybersecurity & Data Privacy Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with cybersecurity & data privacy personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and (3) Document the results of the security testing/evaluation and flaw remediation processes.	5	
ISM-0402	N/A	Applications are comprehensively tested for vulnerabilities, using static application security testing and dynamic application security testing, prior to their initial release and any subsequent releases.				Functional	intersects with	Static Code Analysis	TDA-09.2	Mechanisms exist to require the developers of systems, system components or services to employ static code analysis tools to identify and remediate common flaws and document the results of the analysis.	5	
ISM-0402	N/A	Applications are comprehensively tested for vulnerabilities, using static application security testing and dynamic application security testing, prior to their initial release and any subsequent releases.				Functional	intersects with	Dynamic Code Analysis	TDA-09.3	Mechanisms exist to require the developers of systems, system components or services to employ dynamic code analysis tools to identify and remediate common flaws and document the results of the analysis.	5	
ISM-0402	N/A	Applications are comprehensively tested for vulnerabilities, using static application security testing and dynamic application security testing, prior to their initial release and any subsequent releases.				Functional	intersects with	Malformed Input Testing	TDA-09.4	Mechanisms exist to utilize testing methods to ensure systems, services and products continue to operate as intended when subject to invalid or unexpected inputs on its interfaces.	5	
ISM-0402	N/A	Applications are comprehensively tested for vulnerabilities, using static application security testing and dynamic application security testing, prior to their initial release and any subsequent releases.				Functional	intersects with	Application Penetration Testing	TDA-09.5	Mechanisms exist to perform application-level penetration testing of custom-made applications and services.	5	
ISM-0402	N/A	Applications are comprehensively tested for vulnerabilities, using static application security testing and dynamic application security testing, prior to their initial release and any subsequent releases.				Functional	intersects with	Test Data Integrity	TDA-10.1	Mechanisms exist to ensure the integrity of test data through existing cybersecurity & data privacy controls.	5	
ISM-0405	N/A	Requests for unprivileged access to systems, applications and data repositories are validated when first requested.				Functional	intersects with	Library Privileges	CHG-04.5	Mechanisms exist to restrict software library privileges to those individuals with a pertinent business need for access.	5	
ISM-0405	N/A	Requests for unprivileged access to systems, applications and data repositories are validated when first requested.				Functional	intersects with	Periodic Review of Account Privileges	IAC-17	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	5	
ISM-0405	N/A	Requests for unprivileged access to systems, applications and data repositories are validated when first requested.				Functional	intersects with	Management Approval For New or Changed Accounts	IAC-28.1	Mechanisms exist to ensure management approvals are required for new accounts or changes in permissions to existing accounts.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	Essential 8 ML1	Essential 8 ML1	Essential 8 ML1	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
ISM-0407	N/A	A secure record is maintained for the life of each system covering the following for each user: - their user identification - their signed agreement to abide by usage policies for the system and its resources - who provided authorisation for their access - when their access was granted - the level of access that they were granted - when their access, and their level of access, was last reviewed - when their level of access was changed, and to what extent (if applicable) - when their access was withdrawn (if applicable).				Functional	intersects with	Retain Access Records	IAC-01.1	Mechanisms exist to retain a record of personnel accountability to ensure there is a record of all access granted to an individual (system and application-wise), who provided the authorization, when the authorization was granted and when the access was last reviewed.	5	
ISM-0407	N/A	A secure record is maintained for the life of each system covering the following for each user: - their user identification - their signed agreement to abide by usage policies for the system and its resources - who provided authorisation for their access - when their access was granted - the level of access that they were granted - when their access, and their level of access, was last reviewed - when their level of access was changed, and to what extent (if applicable) - when their access was withdrawn (if applicable).				Functional	intersects with	Audit Trails	MON-03.2	Mechanisms exist to link system access to individual users or service accounts.	5	
ISM-0408	N/A	Systems have a logon banner that reminds users of their security responsibilities when accessing the system and its resources.				Functional	intersects with	System Use Notification (Logon Banner)	SEA-18	Mechanisms exist to utilize system use notification / logon banners that display an approved system use notification message or banner before granting access to the system that provides cybersecurity & data privacy notices.	5	
ISM-0408	N/A	Systems have a logon banner that reminds users of their security responsibilities when accessing the system and its resources.				Functional	intersects with	Standardized Microsoft Windows Banner	SEA-18.1	Mechanisms exist to configure Microsoft Windows-based systems to display an approved logon banner before granting access to the system that provides cybersecurity & data privacy notices.	5	
ISM-0408	N/A	Systems have a logon banner that reminds users of their security responsibilities when accessing the system and its resources.				Functional	intersects with	Truncated Banner	SEA-18.2	Mechanisms exist to utilize a truncated system use notification / logon banner on systems not capable of displaying a logon banner from a centralized source, such as Active Directory.	5	
ISM-0409	N/A	Foreign nationals, including seconded foreign nationals, do not have access to systems that process, store or communicate AUSTEO or REL data unless effective controls are in place to ensure such data is not accessible to them.				Functional	equal	Citizenship Requirements	HRS-04.3	Mechanisms exist to verify that individuals accessing a system processing, storing, or transmitting sensitive information meet applicable statutory, regulatory and/or contractual requirements for citizenship.	10	
ISM-0411	N/A	Foreign nationals, excluding seconded foreign nationals, do not have access to systems that process, store or communicate AGAO data unless effective controls are in place to ensure such data is not accessible to them.				Functional	equal	Citizenship Requirements	HRS-04.3	Mechanisms exist to verify that individuals accessing a system processing, storing, or transmitting sensitive information meet applicable statutory, regulatory and/or contractual requirements for citizenship.	10	
ISM-0414	N/A	Personnel granted access to a system and its resources are uniquely identifiable.				Functional	subset of	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	10	
ISM-0415	N/A	The use of shared user accounts is strictly controlled, and personnel using such accounts are uniquely identifiable.				Functional	intersects with	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
ISM-0415	N/A	The use of shared user accounts is strictly controlled, and personnel using such accounts are uniquely identifiable.				Functional	intersects with	Group Authentication	IAC-02.1	Mechanisms exist to require individuals to be authenticated with an individual authenticator when a group authenticator is utilized.	5	
ISM-0417	N/A	When systems cannot support multi-factor authentication, single-factor authentication using passphrases is implemented instead.				Functional	equal	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	10	
ISM-0418	N/A	Credentials are kept separate from systems they are used to authenticate to, except for when performing authentication activities.				Functional	equal	Protection of Authenticators	IAC-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	10	
ISM-0420	N/A	Where a system processes, stores or communicates AUSTEO, AGAO or REL data, personnel who are foreign nationals are identified as such, including by their specific nationality.				Functional	intersects with	Citizenship Requirements	HRS-04.3	Mechanisms exist to verify that individuals accessing a system processing, storing, or transmitting sensitive information meet applicable statutory, regulatory and/or contractual requirements for citizenship.	5	
ISM-0420	N/A	Where a system processes, stores or communicates AUSTEO, AGAO or REL data, personnel who are foreign nationals are identified as such, including by their specific nationality.				Functional	intersects with	Citizenship Identification	HRS-04.4	Mechanisms exist to identify foreign nationals, including by their specific citizenship.	5	
ISM-0421	N/A	Passphrases used for single-factor authentication are at least 4 random words with a total minimum length of 14 characters, unless more stringent requirements apply.				Functional	intersects with	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	
ISM-0421	N/A	Passphrases used for single-factor authentication are at least 4 random words with a total minimum length of 14 characters, unless more stringent requirements apply.				Functional	intersects with	User Responsibilities for Account Management	IAC-18	Mechanisms exist to compel users to follow accepted practices in the use of authentication mechanisms (e.g., passwords, passphrases, physical or logical security tokens, smart cards, certificates, etc.).	5	
ISM-0422	N/A	Passphrases used for single-factor authentication on TOP SECRET systems are at least 6 random words with a total minimum length of 20 characters.				Functional	intersects with	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	
ISM-0422	N/A	Passphrases used for single-factor authentication on TOP SECRET systems are at least 6 random words with a total minimum length of 20 characters.				Functional	intersects with	User Responsibilities for Account Management	IAC-18	Mechanisms exist to compel users to follow accepted practices in the use of authentication mechanisms (e.g., passwords, passphrases, physical or logical security tokens, smart cards, certificates, etc.).	5	
ISM-0428	N/A	Systems are configured with a session or screen lock that: - activates after a maximum of 15 minutes of user inactivity, or if manually activated by users - conceals all session content on the screen - ensures that the screen does not enter a power saving state before the session or screen lock is activated - requires users to authenticate to unlock the session - denies users the ability to disable the session or screen locking mechanism.				Functional	equal	Session Lock	IAC-24	Mechanisms exist to initiate a session lock after an organization-defined time period of inactivity, or upon receiving a request from a user and retain the session lock until the user reestablishes access using established identification and authentication methods.	10	
ISM-0430	N/A	Access to systems, applications and data repositories is removed or suspended on the same day personnel no longer have a legitimate requirement for access.				Functional	intersects with	Personnel Transfer	HRS-08	Mechanisms exist to adjust logical and physical access authorizations to systems and facilities upon personnel reassignment or transfer, in a timely manner.	5	
ISM-0430	N/A	Access to systems, applications and data repositories is removed or suspended on the same day personnel no longer have a legitimate requirement for access.				Functional	intersects with	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	5	
ISM-0430	N/A	Access to systems, applications and data repositories is removed or suspended on the same day personnel no longer have a legitimate requirement for access.				Functional	intersects with	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	5	
ISM-0430	N/A	Access to systems, applications and data repositories is removed or suspended on the same day personnel no longer have a legitimate requirement for access.				Functional	intersects with	Change of Roles & Duties	IAC-07.1	Mechanisms exist to revoke user access rights following changes in personnel roles and duties, if no longer necessary or permitted.	5	
ISM-0430	N/A	Access to systems, applications and data repositories is removed or suspended on the same day personnel no longer have a legitimate requirement for access.				Functional	intersects with	Termination of Employment	IAC-07.2	Mechanisms exist to revoke user access rights in a timely manner, upon termination of employment or contract.	5	
ISM-0432	N/A	Access requirements for a system and its resources are documented in its system security plan.				Functional	subset of	System Security & Privacy Plan (SSPP)	IAO-03	Mechanisms exist to generate System Security & Privacy Plans (SSPPs), or similar document repositories, to identify and maintain key architectural information on each critical system, application or service, as well as influence inputs, entities, systems, applications and processes, providing a historical record of the data and its origins.	10	
ISM-0434	N/A	Personnel undergo appropriate employment screening and, where necessary, hold an appropriate security clearance before being granted access to a system and its resources.				Functional	equal	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	10	
ISM-0435	N/A	Personnel receive any necessary briefings before being granted access to a system and its resources.				Functional	equal	Formal Indoctrination	HRS-04.2	Mechanisms exist to formally educate authorized users on proper data handling practices for all the relevant types of data to which they have access.	10	
ISM-0441	N/A	When personnel are granted temporary access to a system, effective controls are put in place to restrict their access to only data required for them to undertake their duties.				Functional	intersects with	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	5	
ISM-0441	N/A	When personnel are granted temporary access to a system, effective controls are put in place to restrict their access to only data required for them to undertake their duties.				Functional	intersects with	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
ISM-0443	N/A	Temporary access is not granted to systems that process, store or communicate caveated or sensitive compartmented information.				Functional	subset of	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	10	
ISM-0445	N/A	Privileged users are assigned a dedicated privileged account to be used solely for duties requiring privileged access.	ML1	ML2	ML3	Functional	subset of	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.	10	Essential Eight: ML1, ML2, ML3
ISM-0446	N/A	Foreign nationals, including seconded foreign nationals, do not have privileged access to systems that process, store or communicate AUSTEO or REL data.				Functional	intersects with	Roles With Special Protection Measures	HRS-04.1	Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria.	5	
ISM-0446	N/A	Foreign nationals, including seconded foreign nationals, do not have privileged access to systems that process, store or communicate AUSTEO or REL data.				Functional	intersects with	Citizenship Requirements	HRS-04.3	Mechanisms exist to verify that individuals accessing a system processing, storing, or transmitting sensitive information meet applicable statutory, regulatory and/or contractual requirements for citizenship.	5	
ISM-0446	N/A	Foreign nationals, including seconded foreign nationals, do not have privileged access to systems that process, store or communicate AUSTEO or REL data.				Functional	intersects with	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.	5	
ISM-0447	N/A	Foreign nationals, excluding seconded foreign nationals, do not have privileged access to systems that process, store or communicate AGAO data.				Functional	intersects with	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	Essential 8 ML1	Essential 8 ML1	Essential 8 ML1	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
ISM-0447	N/A	Foreign nationals, excluding seconded foreign nationals, do not have privileged access to systems that process, store or communicate AGAO data.				Functional	intersects with	Citizenship Requirements	HRS-04.3	Mechanisms exist to verify that individuals accessing a system processing, storing, or transmitting sensitive information meet applicable statutory, regulatory and/or contractual requirements for citizenship.	5	
ISM-0447	N/A	Foreign nationals, excluding seconded foreign nationals, do not have privileged access to systems that process, store or communicate AGAO data.				Functional	intersects with	Roles With Special Protection Measures	HRS-04.1	Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria.	5	
ISM-0455	N/A	Where practical, cryptographic equipment and software provides a means of data recovery to allow for circumstances where the encryption key is unavailable due to loss, damage or failure.				Functional	intersects with	Cryptographic Key Loss or Change	CRY-09.3	Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users.	5	
ISM-0455	N/A	Where practical, cryptographic equipment and software provides a means of data recovery to allow for circumstances where the encryption key is unavailable due to loss, damage or failure.				Functional	intersects with	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
ISM-0457	N/A	Cryptographic equipment or software that has completed a Common Criteria evaluation against a Protection Profile is used when encrypting media that contains OFFICIAL: Sensitive or PROTECTED data.				Functional	subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
ISM-0459	N/A	Full disk encryption, or partial encryption where access controls will only allow writing to the encrypted partition, is implemented when encrypting data at rest.				Functional	equal	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	10	
ISM-0460	N/A	HACE is used when encrypting media that contains SECRET or TOP SECRET data.				Functional	subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
ISM-0462	N/A	When a user authenticates to the encryption functionality of IT equipment or media, it is treated in accordance with its original sensitivity or classification until the user deauthenticates from the encryption functionality.				Functional	subset of	Cryptographic Key Loss or Change	CRY-09.3	Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users.	10	
ISM-0465	N/A	Cryptographic equipment or software that has completed a Common Criteria evaluation against a Protection Profile is used to protect OFFICIAL: Sensitive or PROTECTED data when communicated over insufficiently secure networks, outside of appropriately secure areas or via public network infrastructure.				Functional	subset of	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	10	
ISM-0467	N/A	HACE is used to protect SECRET and TOP SECRET data when communicated over insufficiently secure networks, outside of appropriately secure areas or via public network infrastructure.				Functional	subset of	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	10	
ISM-0469	N/A	An ASD-Approved Cryptographic Protocol (AACP) or high assurance cryptographic protocol is used to protect data when communicated over network infrastructure.				Functional	subset of	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	10	
ISM-0471	N/A	Only AACAs or high assurance cryptographic algorithms are used by cryptographic equipment and software.				Functional	subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
ISM-0472	N/A	When using DH for agreeing on encryption session keys, a modulus of at least 2048 bits is used, preferably 3072 bits.				Functional	subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
ISM-0474	N/A	When using ECDH for agreeing on encryption session keys, a base point order and key size of at least 224 bits is used, preferably the NIST P-384 curve.				Functional	subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
ISM-0475	N/A	When using ECDSA for digital signatures, a base point order and key size of at least 224 bits is used, preferably the P-384 curve.				Functional	subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
ISM-0476	N/A	When using RSA for digital signatures, and passing encryption session keys or similar keys, a modulus of at least 2048 bits is used, preferably 3072 bits.				Functional	subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
ISM-0477	N/A	When using RSA for digital signatures, and for passing encryption session keys or similar keys, a different key pair is used for digital signatures and passing encrypted session keys.				Functional	subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
ISM-0479	N/A	Symmetric cryptographic algorithms are not used in Electronic Codebook Mode.				Functional	subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
ISM-0481	N/A	Only AACPs or high assurance cryptographic protocols are used by cryptographic equipment and software.				Functional	subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
ISM-0484	N/A	The SSH daemon is configured to: - only listen on the required interfaces (ListenAddress xxx.xxx.xxx.xxx) - have a suitable login banner (Banner x) - have a login authentication timeout of no more than 60 seconds (LoginGraceTime 60) - disable host-based authentication (HostbasedAuthentication no) - disable rhosts-based authentication (IgnoreRhosts yes) - disable the ability to login directly as root (PermitRootLogin no) - disable empty passwords (PermitEmptyPasswords no) - disable connection forwarding (AllowTCPForwarding no) - disable gateway ports (GatewayPorts no) - disable X11 forwarding (X11Forwarding no).				Functional	subset of	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	10	
ISM-0485	N/A	Public key-based authentication is used for SSH connections.				Functional	subset of	Public Key Infrastructure (PKI)	CRY-08	Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service provider.	10	
ISM-0487	N/A	When using logins without a passphrase for SSH connections, the following are disabled: - access from IP addresses that do not require access - port forwarding - agent credential forwarding - X11 display remoting - console access.				Functional	subset of	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	10	
ISM-0488	N/A	If using remote access without the use of a passphrase for SSH connections, the 'forced command' option is used to specify what command is executed and parameter checking is enabled.				Functional	subset of	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	10	
ISM-0489	N/A	When SSH-agent or similar key caching programs are used, it is limited to workstations and servers with screen locks and key caches that are set to expire within four hours of inactivity.				Functional	subset of	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	10	
ISM-0490	N/A	Versions of S/MIME earlier than S/MIME version 3.0 are not used for S/MIME connections.				Functional	subset of	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	10	
ISM-0494	N/A	Tunnel mode is used for IPsec connections; however, if using transport mode, an IP tunnel is used.				Functional	subset of	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	10	
ISM-0496	N/A	The ESP protocol is used for authentication and encryption of IPsec connections.				Functional	subset of	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	10	
ISM-0498	N/A	A security association lifetime of less than four hours (14400 seconds) is used for IPsec connections.				Functional	subset of	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	10	
ISM-0499	N/A	Communications security doctrine produced by ASD for the management and operation of HACE is complied with.				Functional	subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
ISM-0501	N/A	Keyed cryptographic equipment is transported based on the sensitivity or classification of its keying material.				Functional	subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
ISM-0507	N/A	Cryptographic key management processes, and supporting cryptographic key management procedures, are developed, implemented and maintained.				Functional	equal	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	10	
ISM-0516	N/A	Network documentation includes high-level network diagrams showing all connections into networks and logical network diagrams showing all critical servers, high-value servers, network devices and network security appliances.				Functional	equal	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive/regulated data flows.	10	
ISM-0518	N/A	Network documentation is developed, implemented and maintained.				Functional	subset of	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive/regulated data flows.	10	
ISM-0520	N/A	Network access controls are implemented on networks to prevent the connection of unauthorised network devices and other IT equipment.				Functional	subset of	Network Access Control (NAC)	AST-02.5	Mechanisms exist to maintain a current list of approved technologies (hardware and software).	10	
ISM-0521	N/A	IPv6 functionality is disabled in dual-stack network devices unless it is being used.				Functional	subset of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
ISM-0529	N/A	VLANs are not used to separate network traffic between networks belonging to different security domains.				Functional	equal	Virtual Local Area Network (VLAN) Separation	NET-06.2	Mechanisms exist to enable Virtual Local Area Networks (VLANs) to limit the ability of devices on a network to directly communicate with other devices on the subnet and limit an attacker's ability to laterally move to compromise neighboring systems.	10	
ISM-0530	N/A	Network devices managing VLANs are administered from the most trusted security domain.				Functional	equal	Virtual Local Area Network (VLAN) Separation	NET-06.2	Mechanisms exist to enable Virtual Local Area Networks (VLANs) to limit the ability of devices on a network to directly communicate with other devices on the subnet and limit an attacker's ability to laterally move to compromise neighboring systems.	10	
ISM-0534	N/A	Unused physical ports on network devices are disabled.				Functional	subset of	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	10	
ISM-0535	N/A	Network devices managing VLANs belonging to different security domains do not share VLAN trunks.				Functional	subset of	Virtual Local Area Network (VLAN) Separation	NET-06.2	Mechanisms exist to enable Virtual Local Area Networks (VLANs) to limit the ability of devices on a network to directly communicate with other devices on the subnet and limit an attacker's ability to laterally move to compromise neighboring systems.	10	
ISM-0536	N/A	Public wireless networks provided for general public use are segregated from all other organisation networks.				Functional	intersects with	Guest Networks	NET-02.2	Mechanisms exist to implement and manage a secure guest network.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	Essential 8 ML1	Essential 8 ML1	Essential 8 ML1	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
ISM-0536	N/A	Public wireless networks provided for general public use are segregated from all other organisation networks.				Functional	intersects with	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
ISM-0546	N/A	When video conferencing or IP telephony traffic passes through a gateway containing a firewall or proxy, a video-aware or voice-aware firewall or proxy is used.				Functional	subset of	External Telecommunications Services	NET-03.2	Mechanisms exist to maintain a managed interface for each external telecommunication service that protects the confidentiality and integrity of the information being transmitted across each interface.	10	
ISM-0547	N/A	Video conferencing and IP telephony calls are conducted using a secure real-time transport protocol.				Functional	subset of	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	10	
ISM-0548	N/A	Video conferencing and IP telephony calls are established using a secure session initiation protocol.				Functional	intersects with	Pre/Post Transmission Handling	CRY-01.3	Cryptographic mechanisms exist to ensure the confidentiality and integrity of information during preparation for transmission and during reception.	5	
ISM-0548	N/A	Video conferencing and IP telephony calls are established using a secure session initiation protocol.				Functional	intersects with	Video Teleconference (VTC) Security	AST-20	Mechanisms exist to implement secure Video Teleconference (VTC) capabilities on endpoint devices and in designated conference rooms, to prevent potential eavesdropping.	5	
ISM-0549	N/A	Video conferencing and IP telephony traffic is separated physically or logically from other data traffic.				Functional	subset of	Voice Over Internet Protocol (VoIP) Security	AST-21	Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.	10	
ISM-0551	N/A	IP telephony is configured such that: - IP phones authenticate themselves to the call controller upon registration - auto-registration is disabled and only authorised devices are allowed to access the network - unauthorised devices are blocked by default - all unused and prohibited functionality is disabled.				Functional	intersects with	Video Teleconference (VTC) Security	AST-20	Mechanisms exist to implement secure Video Teleconference (VTC) capabilities on endpoint devices and in designated conference rooms, to prevent potential eavesdropping.	5	
ISM-0551	N/A	IP telephony is configured such that: - IP phones authenticate themselves to the call controller upon registration - auto-registration is disabled and only authorised devices are allowed to access the network - unauthorised devices are blocked by default - all unused and prohibited functionality is disabled.				Functional	intersects with	Voice Over Internet Protocol (VoIP) Security	AST-21	Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.	5	
ISM-0553	N/A	Authentication and authorisation is used for all actions on a video conferencing network, including call setup and changing settings.				Functional	subset of	Video Teleconference (VTC) Security	AST-20	Mechanisms exist to implement secure Video Teleconference (VTC) capabilities on endpoint devices and in designated conference rooms, to prevent potential eavesdropping.	10	
ISM-0554	N/A	An encrypted and non-replayable two-way authentication scheme is used for call authentication and authorisation.				Functional	intersects with	Video Teleconference (VTC) Security	AST-20	Mechanisms exist to implement secure Video Teleconference (VTC) capabilities on endpoint devices and in designated conference rooms, to prevent potential eavesdropping.	5	
ISM-0554	N/A	An encrypted and non-replayable two-way authentication scheme is used for call authentication and authorisation.				Functional	intersects with	Pre/Post Transmission Handling	CRY-01.3	Cryptographic mechanisms exist to ensure the confidentiality and integrity of information during preparation for transmission and during reception.	5	
ISM-0555	N/A	Authentication and authorisation is used for all actions on an IP telephony network, including registering a new IP phone, changing phone users, changing settings and accessing voicemail.				Functional	intersects with	Video Teleconference (VTC) Security	AST-20	Mechanisms exist to implement secure Video Teleconference (VTC) capabilities on endpoint devices and in designated conference rooms, to prevent potential eavesdropping.	5	
ISM-0555	N/A	Authentication and authorisation is used for all actions on an IP telephony network, including registering a new IP phone, changing phone users, changing settings and accessing voicemail.				Functional	intersects with	Voice Over Internet Protocol (VoIP) Security	AST-21	Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.	5	
ISM-0556	N/A	Workstations are not connected to video conferencing units or IP phones unless the workstation or the device uses Virtual Local Area Networks or similar mechanisms to maintain separation between video conferencing, IP telephony and other data traffic.				Functional	subset of	Voice Over Internet Protocol (VoIP) Security	AST-21	Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.	10	
ISM-0558	N/A	IP phones used in public areas do not have the ability to access data networks, voicemail and directory services.				Functional	intersects with	Telecommunications Equipment	AST-19	Mechanisms exist to establish usage restrictions and implementation guidance for telecommunication equipment to prevent potential damage or unauthorized modification and to prevent potential eavesdropping.	5	
ISM-0558	N/A	IP phones used in public areas do not have the ability to access data networks, voicemail and directory services.				Functional	intersects with	Voice Over Internet Protocol (VoIP) Security	AST-21	Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.	5	
ISM-0559	N/A	Microphones (including headsets and USB handsets) and webcams are not used with non-SECRET workstations in SECRET areas.				Functional	subset of	Microphones & Web Cameras	AST-22	Mechanisms exist to configure assets to prohibit the use of endpoint-based microphones and web cameras in secure areas or where sensitive/regulated information is discussed.	10	
ISM-0565	N/A	Email servers are configured to block, log and report emails with inappropriate protective markings.				Functional	subset of	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	10	
ISM-0567	N/A	Email servers only relay emails destined for or originating from their domains (including subdomains).				Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
ISM-0567	N/A	Email servers only relay emails destined for or originating from their domains (including subdomains).				Functional	intersects with	Adaptive Email Protections	NET-20.7	Mechanisms exist to utilize adaptive email protections that involve employing risk-based analysis in the application and enforcement of email protections.	5	
ISM-0569	N/A	Emails are routed via centralised email gateways.				Functional	subset of	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	10	
ISM-0570	N/A	Where backup or alternative email gateways are in place, they are maintained at the same standard as the primary email gateway.				Functional	intersects with	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
ISM-0570	N/A	Where backup or alternative email gateways are in place, they are maintained at the same standard as the primary email gateway.				Functional	intersects with	Route Internal Traffic to Proxy Servers	NET-18.1	Mechanisms exist to route internal communications traffic to external networks through organization-approved proxy servers at managed interfaces.	5	
ISM-0571	N/A	When users send or receive emails, an authenticated and encrypted channel is used to route emails via their organisation's centralised email gateways.				Functional	subset of	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	10	
ISM-0572	N/A	Opportunistic TLS encryption is enabled on email servers that make incoming or outgoing email connections over public network infrastructure.				Functional	subset of	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	10	
ISM-0574	N/A	SPF is used to specify authorised email servers (or lack thereof) for an organisation's domains (including subdomains).				Functional	intersects with	Domain Name Service (DNS) Resolution	NET-10	Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.	5	
ISM-0574	N/A	SPF is used to specify authorised email servers (or lack thereof) for an organisation's domains (including subdomains).				Functional	intersects with	Sender Policy Framework (SPF)	NET-10.3	Mechanisms exist to validate the legitimacy of email communications through configuring a Domain Naming Service (DNS) Sender Policy Framework (SPF) record to specify the IP addresses and/or hostnames that are authorized to send email from the specified domain.	5	
ISM-0574	N/A	SPF is used to specify authorised email servers (or lack thereof) for an organisation's domains (including subdomains).				Functional	intersects with	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
ISM-0576	N/A	A cyber security incident management policy, and associated cyber security incident response plan, is developed, implemented and maintained.				Functional	subset of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	10	
ISM-0576	N/A	A cyber security incident management policy, and associated cyber security incident response plan, is developed, implemented and maintained.				Functional	intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
ISM-0580	N/A	An event logging policy is developed, implemented and maintained.				Functional	subset of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
ISM-0582	N/A	The following events are centrally logged for operating systems: - application and operating system crashes and error messages - changes to security policies and system configurations - successful user logons and logoffs, failed user logons and account lockouts - failures, restarts and changes to important processes and services - requests to access internet resources - security product-related events - system startups and shutdowns.				Functional	equal	Content of Event Logs	MON-03	Mechanisms exist to configure systems to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	10	
ISM-0585	N/A	For each event logged, the date and time of the event, the relevant user or process, the relevant filename, the event description, and the IT equipment involved are recorded.				Functional	equal	Content of Event Logs	MON-03	Mechanisms exist to configure systems to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	10	
ISM-0588	N/A	A fax machine and MFD usage policy is developed, implemented and maintained.				Functional	subset of	Use of Communications Technology	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously.	10	
ISM-0589	N/A	MFDs are not used to scan or copy documents above the sensitivity or classification of networks they are connected to.				Functional	subset of	Multi-Function Devices (MFD)	AST-23	Mechanisms exist to securely configure Multi-Function Devices (MFD) according to industry-recognized secure practices for the type of device.	10	
ISM-0590	N/A	Authentication measures for MFDs are the same strength as those used for workstations on networks they are connected to.				Functional	subset of	Multi-Function Devices (MFD)	AST-23	Mechanisms exist to securely configure Multi-Function Devices (MFD) according to industry-recognized secure practices for the type of device.	10	
ISM-0591	N/A	Evaluated peripheral switches are used when sharing peripherals between systems.				Functional	subset of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
ISM-0597	N/A	When planning, designing, implementing or introducing additional connectivity to CDSs, ASD is consulted and any directions provided by ASD are complied with.				Functional	subset of	Cross Domain Solution (CDS)	NET-02.3	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	10	
ISM-0610	N/A	Users are trained on the secure use of CDSs before access is granted.				Functional	subset of	Cross Domain Solution (CDS)	NET-02.3	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	10	
ISM-0611	N/A	System administrators for gateways are assigned the minimum privileges required to perform their duties.				Functional	intersects with	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
ISM-0611	N/A	System administrators for gateways are assigned the minimum privileges required to perform their duties.				Functional	intersects with	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
ISM-0612	N/A	System administrators for gateways are formally trained on the operation and management of gateways.				Functional	subset of	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	Essential 8 ML1	Essential 8 ML1	Essential 8 ML1	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
ISM-0613	N/A	System administrators for gateways that connect to Australian Eyes Only or Releasable To networks are Australian nationals.				Functional	subset of	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	10	
ISM-0616	N/A	Separation of duties is implemented in performing administrative activities for gateways.				Functional	subset of	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	10	
ISM-0619	N/A	Users authenticate to other networks accessed via gateways.				Functional	subset of	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	10	
ISM-0622	N/A	IT equipment authenticates to other networks accessed via gateways.				Functional	subset of	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	10	
ISM-0626	N/A	CDSs are implemented between SECRET or TOP SECRET networks and any other networks belonging to different security domains.				Functional	subset of	Cross Domain Solution (CDS)	NET-02.3	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	10	
ISM-0628	N/A	Gateways are implemented between networks belonging to different security domains.				Functional	subset of	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	10	
ISM-0629	N/A	For gateways between networks belonging to different security domains, any shared components are managed by system administrators for the higher security domain or by system administrators from a mutually agreed upon third party.				Functional	subset of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
ISM-0629	N/A	For gateways between networks belonging to different security domains, any shared components are managed by system administrators for the higher security domain or by system administrators from a mutually agreed upon third party.				Functional	intersects with	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
ISM-0631	N/A	Gateways only allow explicitly authorised data flows.				Functional	subset of	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	10	
ISM-0634	N/A	The following events are centrally logged for gateways: - data packets and data flows permitted through gateways - data packets and data flows attempting to leave gateways - real-time alerts for attempted intrusions.				Functional	subset of	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	10	
ISM-0635	N/A	CDSs implement isolated upward and downward network paths.				Functional	subset of	Cross Domain Solution (CDS)	NET-02.3	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	10	
ISM-0637	N/A	Gateways implement a demilitarised zone if external parties require access to an organisation's services.				Functional	intersects with	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
ISM-0637	N/A	Gateways implement a demilitarised zone if external parties require access to an organisation's services.				Functional	intersects with	DMZ Networks	NET-08.1	Mechanisms exist to monitor De-Militarized Zone (DMZ) network segments to separate untrusted networks from trusted networks.	5	
ISM-0639	N/A	Evaluated firewalls are used between networks belonging to different security domains.				Functional	subset of	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	10	
ISM-0643	N/A	Evaluated diodes are used for controlling the data flow of unidirectional gateways between an organisation's networks and public network infrastructure.				Functional	subset of	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	10	
ISM-0645	N/A	Evaluated diodes used for controlling the data flow of unidirectional gateways between SECRET or TOP SECRET networks and public network infrastructure complete a high assurance evaluation.				Functional	subset of	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	10	
ISM-0649	N/A	Files imported or exported via gateways or CDSs are filtered for allowed file types.				Functional	subset of	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	10	
ISM-0651	N/A	Files identified by content filtering checks as malicious, or that cannot be inspected, are blocked.				Functional	subset of	Detonation Chambers (Sandboxes)	IRO-15	Mechanisms exist to utilize a detonation chamber capability to detect and/or block potentially-malicious files and email attachments.	10	
ISM-0652	N/A	Files identified by content filtering checks as suspicious are quarantined until reviewed and subsequently approved or not approved for release.				Functional	subset of	Detonation Chambers (Sandboxes)	IRO-15	Mechanisms exist to utilize a detonation chamber capability to detect and/or block potentially-malicious files and email attachments.	10	
ISM-0657	N/A	When manually importing data to systems, the data is scanned for malicious and active content.				Functional	subset of	Information Sharing	DCH-14	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	10	
ISM-0659	N/A	Files imported or exported via gateways or CDSs undergo content filtering checks.				Functional	subset of	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	10	
ISM-0660	N/A	Data transfer logs for SECRET and TOP SECRET systems are fully verified at least monthly.				Functional	subset of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
ISM-0661	N/A	Users transferring data to and from systems are held accountable for data transfers they perform.				Functional	subset of	Information Sharing	DCH-14	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	10	
ISM-0663	N/A	Data transfer processes, and supporting data transfer procedures, are developed, implemented and maintained.				Functional	subset of	Information Sharing	DCH-14	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	10	
ISM-0664	N/A	Data exported from SECRET and TOP SECRET systems is reviewed and authorised by a trusted source beforehand.				Functional	subset of	Information Sharing	DCH-14	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	10	
ISM-0665	N/A	Trusted sources for SECRET and TOP SECRET systems are limited to people and services that have been authorised as such by the Chief Information Security Officer.				Functional	intersects with	Information Sharing	DCH-14	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	5	
ISM-0665	N/A	Trusted sources for SECRET and TOP SECRET systems are limited to people and services that have been authorised as such by the Chief Information Security Officer.				Functional	intersects with	Zero Trust Architecture (ZTA)	NET-01.1	Mechanisms exist to treat all users and devices as potential threats and prevent access to data and resources until the users can be properly authenticated and their access authorized.	5	
ISM-0669	N/A	When manually exporting data from SECRET and TOP SECRET systems, digital signatures are validated and keyword checks are performed within all textual data.				Functional	subset of	Information Sharing	DCH-14	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	10	
ISM-0670	N/A	All security-relevant events generated by CDSs are centrally logged.				Functional	subset of	Cross Domain Solution (CDS)	NET-02.3	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	10	
ISM-0675	N/A	Data authorised for export from SECRET and TOP SECRET systems is digitally signed by a trusted source.				Functional	subset of	Information Sharing	DCH-14	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	10	
ISM-0677	N/A	Files imported or exported via gateways or CDSs that have a digital signature or cryptographic checksum are validated.				Functional	subset of	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	10	
ISM-0682	N/A	Bluetooth functionality is not enabled on SECRET and TOP SECRET mobile devices.				Functional	subset of	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	10	
ISM-0687	N/A	Mobile devices that access SECRET or TOP SECRET systems or data use mobile platforms that have been issued an Approval for Use by ASD and are operated in accordance with the latest version of their associated Australian Communications Security Instruction.				Functional	subset of	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	10	
ISM-0694	N/A	Privately-owned mobile devices and desktop computers do not access SECRET and TOP SECRET systems or data.				Functional	subset of	Personally-Owned Mobile Devices	MDM-06	Mechanisms exist to restrict the connection of personally-owned, mobile devices to organizational systems and networks.	10	
ISM-0701	N/A	Mobile device emergency sanitisation processes, and supporting mobile device emergency sanitisation procedures, are developed, implemented and maintained.				Functional	intersects with	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
ISM-0701	N/A	Mobile device emergency sanitisation processes, and supporting mobile device emergency sanitisation procedures, are developed, implemented and maintained.				Functional	intersects with	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
ISM-0702	N/A	If a cryptographic zeroise or sanitise function is provided for cryptographic keys on a SECRET or TOP SECRET mobile device, the function is used as part of mobile device emergency sanitisation processes and procedures.				Functional	subset of	Remote Purging	MDM-05	Mechanisms exist to remotely purge selected information from mobile devices.	10	
ISM-0705	N/A	When accessing an organisation's network via a VPN connection, split tunnelling is disabled.				Functional	intersects with	Split Tunneling	CFG-03.4	Mechanisms exist to prevent split tunneling for remote devices unless the split tunnel is securely provisioned using organization-defined safeguards.	5	
ISM-0705	N/A	When accessing an organisation's network via a VPN connection, split tunnelling is disabled.				Functional	intersects with	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
ISM-0714	N/A	A CISO is appointed to provide cyber security leadership and guidance for their organisation.				Functional	equal	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	10	
ISM-0717	N/A	The CISO oversees the management of cyber security personnel within their organisation.				Functional	intersects with	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
ISM-0717	N/A	The CISO oversees the management of cyber security personnel within their organisation.				Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
ISM-0718	N/A	The CISO regularly reports directly to their organisation's executive committee or board of directors on cyber security matters.				Functional	equal	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.	10	
ISM-0720	N/A	The CISO oversees the development, implementation and maintenance of a cyber security communications strategy to assist in communicating the cyber security vision and strategy for their organisation.				Functional	intersects with	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
ISM-0720	N/A	The CISO oversees the development, implementation and maintenance of a cyber security communications strategy to assist in communicating the cyber security vision and strategy for their organisation.				Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	Essential 8 ML1	Essential 8 ML1	Essential 8 ML1	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
ISM-0720	N/A	The CISO oversees the development, implementation and maintenance of a cyber security communications strategy to assist in communicating the cyber security vision and strategy for their organisation.				Functional	subset of	Cybersecurity & Data Privacy Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy-related resource planning controls that define a viable plan for achieving cybersecurity & data privacy objectives.	10	
ISM-0720	N/A	The CISO oversees the development, implementation and maintenance of a cyber security communications strategy to assist in communicating the cyber security vision and strategy for their organisation.				Functional	intersects with	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a strategic cybersecurity & data privacy-specific business plan and set of objectives to achieve that plan.	5	
ISM-0720	N/A	The CISO oversees the development, implementation and maintenance of a cyber security communications strategy to assist in communicating the cyber security vision and strategy for their organisation.				Functional	intersects with	Cybersecurity & Data Privacy Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical systems, system components or services at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
ISM-0720	N/A	The CISO oversees the development, implementation and maintenance of a cyber security communications strategy to assist in communicating the cyber security vision and strategy for their organisation.				Functional	subset of	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
ISM-0724	N/A	The CISO implements cyber security measurement metrics and key performance indicators for their organisation.				Functional	intersects with	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
ISM-0724	N/A	The CISO implements cyber security measurement metrics and key performance indicators for their organisation.				Functional	intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	5	
ISM-0724	N/A	The CISO implements cyber security measurement metrics and key performance indicators for their organisation.				Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
ISM-0725	N/A	The CISO coordinates cyber security and business alignment through a cyber security steering committee or advisory board, comprising of key cyber security and business executives, which meets formally and on a regular basis.				Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
ISM-0725	N/A	The CISO coordinates cyber security and business alignment through a cyber security steering committee or advisory board, comprising of key cyber security and business executives, which meets formally and on a regular basis.				Functional	intersects with	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
ISM-0725	N/A	The CISO coordinates cyber security and business alignment through a cyber security steering committee or advisory board, comprising of key cyber security and business executives, which meets formally and on a regular basis.				Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
ISM-0726	N/A	The CISO coordinates security risk management activities between cyber security and business teams.				Functional	intersects with	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
ISM-0726	N/A	The CISO coordinates security risk management activities between cyber security and business teams.				Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
ISM-0726	N/A	The CISO coordinates security risk management activities between cyber security and business teams.				Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
ISM-0731	N/A	The CISO oversees cyber supply chain risk management activities for their organisation.				Functional	intersects with	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
ISM-0731	N/A	The CISO oversees cyber supply chain risk management activities for their organisation.				Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
ISM-0731	N/A	The CISO oversees cyber supply chain risk management activities for their organisation.				Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
ISM-0731	N/A	The CISO oversees cyber supply chain risk management activities for their organisation.				Functional	intersects with	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with the services and product supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5	
ISM-0732	N/A	The CISO receives and manages a dedicated cyber security budget for their organisation.				Functional	intersects with	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
ISM-0732	N/A	The CISO receives and manages a dedicated cyber security budget for their organisation.				Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
ISM-0732	N/A	The CISO receives and manages a dedicated cyber security budget for their organisation.				Functional	subset of	Cybersecurity & Data Privacy Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy-related resource planning controls that define a viable plan for achieving cybersecurity & data privacy objectives.	10	
ISM-0732	N/A	The CISO receives and manages a dedicated cyber security budget for their organisation.				Functional	intersects with	Cybersecurity & Data Privacy Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the cybersecurity & data privacy programs and document all exceptions to this requirement.	5	
ISM-0732	N/A	The CISO receives and manages a dedicated cyber security budget for their organisation.				Functional	intersects with	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data privacy requirements within business process planning for projects / initiatives.	5	
ISM-0733	N/A	The CISO is fully aware of all cyber security incidents within their organisation.				Functional	intersects with	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
ISM-0733	N/A	The CISO is fully aware of all cyber security incidents within their organisation.				Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
ISM-0733	N/A	The CISO is fully aware of all cyber security incidents within their organisation.				Functional	intersects with	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity & data privacy incident response operations.	5	
ISM-0733	N/A	The CISO is fully aware of all cyber security incidents within their organisation.				Functional	intersects with	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity & data privacy incidents to internal stakeholders all the way through the resolution of the incident.	5	
ISM-0733	N/A	The CISO is fully aware of all cyber security incidents within their organisation.				Functional	intersects with	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.	5	
ISM-0733	N/A	The CISO is fully aware of all cyber security incidents within their organisation.				Functional	intersects with	Cyber Incident Reporting for Sensitive Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	5	
ISM-0734	N/A	The CISO contributes to the development, implementation and maintenance of business continuity and disaster recovery plans for their organisation to ensure that business-critical services are supported appropriately in the event of a disaster.				Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
ISM-0734	N/A	The CISO contributes to the development, implementation and maintenance of business continuity and disaster recovery plans for their organisation to ensure that business-critical services are supported appropriately in the event of a disaster.				Functional	intersects with	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
ISM-0734	N/A	The CISO contributes to the development, implementation and maintenance of business continuity and disaster recovery plans for their organisation to ensure that business-critical services are supported appropriately in the event of a disaster.				Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
ISM-0735	N/A	The CISO oversees the development, implementation and maintenance of their organisation's cyber security awareness training program.				Functional	intersects with	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
ISM-0735	N/A	The CISO oversees the development, implementation and maintenance of their organisation's cyber security awareness training program.				Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
ISM-0735	N/A	The CISO oversees the development, implementation and maintenance of their organisation's cyber security awareness training program.				Functional	subset of	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
ISM-0810	N/A	Systems are secured in facilities that meet the requirements for a security zone suitable for their classification.				Functional	subset of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
ISM-0813	N/A	Server rooms, communications rooms, security containers and secure rooms are not left in unsecured states.				Functional	subset of	Access To Information Systems	PES-03.4	Physical access control mechanisms exist to enforce physical access to critical information systems or sensitive/regulated data, in addition to the physical access controls for the facility.	10	
ISM-0817	N/A	Personnel are advised of what suspicious contact via online services is and how to report it.				Functional	intersects with	Social Engineering & Mining	SAT-02.2	Mechanisms exist to include awareness training on recognizing and reporting potential and actual instances of social engineering and social mining.	5	
ISM-0817	N/A	Personnel are advised of what suspicious contact via online services is and how to report it.				Functional	intersects with	Suspicious Communications & Anomalous System Behavior	SAT-03.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.	5	
ISM-0820	N/A	Personnel are advised to not post work information to unauthorised online services and to report cases where such information is posted.				Functional	subset of	Social Media & Social Networking Restrictions	HRS-05.2	Mechanisms exist to define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information.	10	
ISM-0821	N/A	Personnel are advised of security risks associated with posting personal information to online services and are encouraged to use any available privacy settings to restrict who can view such information.				Functional	subset of	Social Media & Social Networking Restrictions	HRS-05.2	Mechanisms exist to define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information.	10	
ISM-0824	N/A	Personnel are advised not to send or receive files via unauthorised online services.				Functional	intersects with	Unsupported Internet Browsers & Email Clients	CFG-04.2	Mechanisms exist to allow only approved Internet browsers and email clients to run on systems.	5	
ISM-0824	N/A	Personnel are advised not to send or receive files via unauthorised online services.				Functional	intersects with	User Awareness	HRS-03.1	Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	Essential 8 ML1	Essential 8 ML1	Essential 8 ML1	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
ISM-0824	N/A	Personnel are advised not to send or receive files via unauthorised online services.				Functional	intersects with	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	
ISM-0824	N/A	Personnel are advised not to send or receive files via unauthorised online services.				Functional	intersects with	Use of Communications Technology	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously.	5	
ISM-0824	N/A	Personnel are advised not to send or receive files via unauthorised online services.				Functional	intersects with	Cybersecurity & Data Privacy Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	
ISM-0824	N/A	Personnel are advised not to send or receive files via unauthorised online services.				Functional	intersects with	Suspicious Communications & Anomalous System Behavior	SAT-03.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.	5	
ISM-0829	N/A	Security measures are used to detect and respond to unauthorised RF devices in SECRET and TOP SECRET areas.				Functional	subset of	Rogue Wireless Detection	NET-15.5	Mechanisms exist to test for the presence of Wireless Access Points (WAPs) and identify all authorized and unauthorized WAPs within the facility(ies).	10	
ISM-0831	N/A	Media is handled in a manner suitable for its sensitivity or classification.				Functional	subset of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
ISM-0831	N/A	Media is handled in a manner suitable for its sensitivity or classification.				Functional	intersects with	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive / regulated data is formally trained in data handling requirements.	5	
ISM-0835	N/A	Following sanitisation, TOP SECRET volatile media retains its classification if it stored static data for an extended period of time, or had data repeatedly stored on or written to the same memory location for an extended period of time.				Functional	subset of	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	10	
ISM-0836	N/A	Non-volatile EEPROM media is sanitised by overwriting it at least once in its entirety with a random pattern followed by a read back for verification.				Functional	subset of	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	10	
ISM-0839	N/A	The destruction of media storing accountable material is not outsourced.				Functional	intersects with	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
ISM-0839	N/A	The destruction of media storing accountable material is not outsourced.				Functional	intersects with	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
ISM-0840	N/A	When outsourcing the destruction of media storing non-accountable material, a National Association for Information Destruction AAA certified destruction service with endorsements, as specified in ASIO's Protective Security Circular-167, is used.				Functional	subset of	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	10	
ISM-0843	N/A	Application control is implemented on workstations.	ML1	ML2	ML3	Functional	intersects with	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5	Essential Eight: ML1, ML2, ML3
ISM-0843	N/A	Application control is implemented on workstations.	ML1	ML2	ML3	Functional	intersects with	Configuration Enforcement	CFG-06	Automated mechanisms exist to monitor, enforce and report on configurations for endpoint devices.	5	Essential Eight: ML1, ML2, ML3
ISM-0843	N/A	Application control is implemented on workstations.	ML1	ML2	ML3	Functional	intersects with	Integrity Assurance & Enforcement (IAE)	CFG-06.1	Automated mechanisms exist to identify unauthorized deviations from an approved baseline and implement automated resiliency actions to remediate the unauthorized change.	5	Essential Eight: ML1, ML2, ML3
ISM-0846	N/A	All users (with the exception of local administrator accounts and break glass accounts) cannot disable, bypass or be exempted from application control.				Functional	intersects with	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5	
ISM-0846	N/A	All users (with the exception of local administrator accounts and break glass accounts) cannot disable, bypass or be exempted from application control.				Functional	intersects with	Configuration Enforcement	CFG-06	Automated mechanisms exist to monitor, enforce and report on configurations for endpoint devices.	5	
ISM-0846	N/A	All users (with the exception of local administrator accounts and break glass accounts) cannot disable, bypass or be exempted from application control.				Functional	intersects with	Integrity Assurance & Enforcement (IAE)	CFG-06.1	Automated mechanisms exist to identify unauthorized deviations from an approved baseline and implement automated resiliency actions to remediate the unauthorized change.	5	
ISM-0853	N/A	On a daily basis, outside of business hours and after an appropriate period of inactivity, user sessions are terminated and workstations are restarted.				Functional	subset of	Session Termination	IAC-25	Automated mechanisms exist to log out users, both locally on the network and for remote sessions, at the end of the session or after an organization-defined period of inactivity.	10	
ISM-0854	N/A	AUSTEO and AGAO data can only be accessed from systems under the sole control of the Australian Government that are located within facilities authorised by the Australian Government.				Functional	subset of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
ISM-0859	N/A	Event logs, excluding those for Domain Name System services and web proxies, are retained for at least seven years.				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 satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
ISM-0859	N/A	Event logs, excluding those for Domain Name System services and web proxies, are retained for at least seven years.				Functional	intersects with	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	
ISM-0859	N/A	Event logs, excluding those for Domain Name System services and web proxies, are retained for at least seven years.				Functional	intersects with	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	5	
ISM-0859	N/A	Event logs, excluding those for Domain Name System services and web proxies, are retained for at least seven years.				Functional	intersects with	Event Log Retention	MON-10	Mechanisms exist to retain event logs for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	5	
ISM-0861	N/A	DKIM signing is enabled on emails originating from an organisation's domains (including subdomains).				Functional	intersects with	Domain Name Service (DNS) Resolution	NET-10	Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.	5	
ISM-0861	N/A	DKIM signing is enabled on emails originating from an organisation's domains (including subdomains).				Functional	intersects with	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
ISM-0863	N/A	Mobile devices prevent personnel from installing non-approved applications once provisioned.				Functional	subset of	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	10	
ISM-0864	N/A	Mobile devices prevent personnel from disabling or modifying security functionality once provisioned.				Functional	subset of	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	10	
ISM-0866	N/A	Sensitive or classified data is not viewed or communicated in public locations unless care is taken to reduce the chance of the screen of a mobile device being observed.				Functional	subset of	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	10	
ISM-0869	N/A	Mobile devices encrypt their internal storage and any removable media.				Functional	subset of	Full Device & Container-Based Encryption	MDM-03	Cryptographic mechanisms exist to protect the confidentiality and integrity of information on mobile devices through full-device or container encryption.	10	
ISM-0870	N/A	Mobile devices are carried or stored in a secured state when not being actively used.				Functional	subset of	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	10	
ISM-0871	N/A	Mobile devices are kept under continual direct supervision when being actively used.				Functional	subset of	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	10	
ISM-0874	N/A	Mobile devices and desktop computers access the internet via a VPN connection to an organisation's internet gateway rather than via a direct connection to the internet.				Functional	intersects with	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
ISM-0874	N/A	Mobile devices and desktop computers access the internet via a VPN connection to an organisation's internet gateway rather than via a direct connection to the internet.				Functional	subset of	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	10	
ISM-0888	N/A	Security documentation is reviewed at least annually and includes a 'current as at [date]' or equivalent statement.				Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
ISM-0888	N/A	Security documentation is reviewed at least annually and includes a 'current as at [date]' or equivalent statement.				Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
ISM-0917	N/A	When malicious code is detected, the following steps are taken to handle the infection: - the infected systems are isolated - all previously connected media used in the period leading up to the infection are scanned for signs of infection and isolated if necessary - antivirus software is used to remove the infection from infected systems and media - if the infection cannot be reliably removed, systems are restored from a known good backup or rebuilt.				Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
ISM-0917	N/A	When malicious code is detected, the following steps are taken to handle the infection: - the infected systems are isolated - all previously connected media used in the period leading up to the infection are scanned for signs of infection and isolated if necessary - antivirus software is used to remove the infection from infected systems and media - if the infection cannot be reliably removed, systems are restored from a known good backup or rebuilt.				Functional	intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
ISM-0926	N/A	OFFICIAL: Sensitive and PROTECTED cables are coloured neither salmon pink nor red.				Functional	subset of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
ISM-0931	N/A	In SECRET and TOP SECRET areas, push-to-talk handsets or push-to-talk headsets are used to meet any off-hook audio protection requirements.				Functional	subset of	Use of Communications Technology	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously.	10	
ISM-0938	N/A	User applications are chosen from vendors that have demonstrated a commitment to secure-by-design and secure-by- default principles, use of memory-safe programming languages where possible, secure programming practices, and maintaining the security of their products.				Functional	subset of	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10	
ISM-0947	N/A	When transferring data manually between two systems belonging to different security domains, rewritable media is sanitised after each data transfer.				Functional	intersects with	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
ISM-0947	N/A	When transferring data manually between two systems belonging to different security domains, rewritable media is sanitised after each data transfer.				Functional	intersects with	Ad-Hoc Transfers	DCH-17	Mechanisms exist to secure ad-hoc exchanges of large digital files with internal or external parties.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	Essential 8 ML1	Essential 8 ML1	Essential 8 ML1	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
ISM-0955	N/A	Application control is implemented using cryptographic hash rules, publisher certificate rules or path rules.				Functional	intersects with	Configuration Enforcement	CFG-06	Automated mechanisms exist to monitor, enforce and report on configurations for endpoint devices.	5	
ISM-0955	N/A	Application control is implemented using cryptographic hash rules, publisher certificate rules or path rules.				Functional	intersects with	Integrity Assurance & Enforcement (IAE)	CFG-06.1	Automated mechanisms exist to identify unauthorized deviations from an approved baseline and implement automated resiliency actions to remediate the unauthorized change.	5	
ISM-0958	N/A	An organisation-approved list of domain names, or list of website categories, is implemented for all Hypertext Transfer Protocol and Hypertext Transfer Protocol Secure traffic communicated through gateways.				Functional	subset of	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	10	
ISM-0961	N/A	Client-side active content is restricted by web content filters to an organisation-approved list of domain names.				Functional	subset of	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	10	
ISM-0963	N/A	Web content filtering is implemented to filter potentially harmful web-based content.				Functional	subset of	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	10	
ISM-0971	N/A	The OWASP Application Security Verification Standard is used in the development of web applications.				Functional	subset of	Web Security Standard	WEB-07	Mechanisms exist to ensure the Open Web Application Security Project (OWASP) Application Security Verification Standard is incorporated into the organization's Secure Systems Development Lifecycle (SSDLC) process.	10	
ISM-0974	N/A	Multi-factor authentication is used to authenticate unprivileged users of systems.		ML2	ML3	Functional	equal	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	10	Essential Eight: ML2, ML3
ISM-0988	N/A	An accurate time source is established and used consistently across systems to assist with identifying connections between events.				Functional	intersects with	System-Wide / Time-Correlated Audit Trail	MON-02.7	Automated mechanisms exist to compile audit records into an organization-wide audit trail that is time-correlated.	5	
ISM-0988	N/A	An accurate time source is established and used consistently across systems to assist with identifying connections between events.				Functional	intersects with	Clock Synchronization	SEA-20	Mechanisms exist to utilize time-synchronization technology to synchronize all critical system clocks.	5	
ISM-0991	N/A	Event logs for Domain Name System services and web proxies are retained for at least 18 months.				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 satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
ISM-0991	N/A	Event logs for Domain Name System services and web proxies are retained for at least 18 months.				Functional	intersects with	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	
ISM-0991	N/A	Event logs for Domain Name System services and web proxies are retained for at least 18 months.				Functional	intersects with	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	5	
ISM-0991	N/A	Event logs for Domain Name System services and web proxies are retained for at least 18 months.				Functional	intersects with	Event Log Retention	MON-10	Mechanisms exist to retain event logs for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	5	
ISM-0994	N/A	ECDH is used in preference to DH.				Functional	subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
ISM-0998	N/A	AUTH_HMAC_SHA2_256_128, AUTH_HMAC_SHA2_384_192, AUTH_HMAC_SHA2_512_256 or NONE (only with AES-GCM) is used for authenticating IPsec connections, preferably NONE.				Functional	subset of	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	10	
ISM-0999	N/A	DH or ECDH is used for key establishment of IPsec connections, preferably 384-bit random ECP group, 3072-bit MODP Group or 4096-bit MODP Group.				Functional	subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
ISM-0999	N/A	DH or ECDH is used for key establishment of IPsec connections, preferably 384-bit random ECP group, 3072-bit MODP Group or 4096-bit MODP Group.				Functional	intersects with	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
ISM-1000	N/A	PFS is used for IPsec connections.				Functional	subset of	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	10	
ISM-1006	N/A	Security measures are implemented to prevent unauthorised access to network management traffic.				Functional	intersects with	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5	
ISM-1006	N/A	Security measures are implemented to prevent unauthorised access to network management traffic.				Functional	intersects with	Restrict Access To Security Functions	END-16	Mechanisms exist to ensure security functions are restricted to authorized individuals and enforce least privilege control requirements for necessary job functions.	5	
ISM-1013	N/A	The effective range of wireless communications outside an organisation's area of control is limited by implementing RF shielding on facilities in which SECRET or TOP SECRET wireless networks are used.				Functional	subset of	Wireless Boundaries	NET-15.4	Mechanisms exist to confine wireless communications to organization-controlled boundaries.	10	
ISM-1014	N/A	Individual logins are implemented for IP phones used for SECRET or TOP SECRET conversations.				Functional	intersects with	Video Teleconference (VTC) Security	AST-20	Mechanisms exist to implement secure Video Teleconference (VTC) capabilities on endpoint devices and in designated conference rooms, to prevent potential eavesdropping.	5	
ISM-1014	N/A	Individual logins are implemented for IP phones used for SECRET or TOP SECRET conversations.				Functional	intersects with	Voice Over Internet Protocol (VoIP) Security	AST-21	Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.	5	
ISM-1019	N/A	A denial of service response plan for video conferencing and IP telephony services is developed, implemented and maintained.				Functional	subset of	Denial of Service (DoS) Protection	NET-02.1	Automated mechanisms exist to protect against or limit the effects of denial of service attacks.	10	
ISM-1023	N/A	The intended recipients of blocked inbound emails, and the senders of blocked outbound emails, are notified.				Functional	subset of	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	10	
ISM-1024	N/A	Notifications of undeliverable emails are only sent to senders that can be verified via SPF or other trusted means.				Functional	subset of	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	10	
ISM-1026	N/A	DKIM signatures on incoming emails are verified.				Functional	intersects with	Domain Name Service (DNS) Resolution	NET-10	Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.	5	
ISM-1026	N/A	DKIM signatures on incoming emails are verified.				Functional	intersects with	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
ISM-1027	N/A	Email distribution list software used by external senders is configured such that it does not break the validity of the sender's DKIM signature.				Functional	intersects with	Domain Name Service (DNS) Resolution	NET-10	Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.	5	
ISM-1027	N/A	Email distribution list software used by external senders is configured such that it does not break the validity of the sender's DKIM signature.				Functional	intersects with	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
ISM-1028	N/A	A NIDS or NIPS is deployed in gateways between an organisation's networks and other networks they do not manage.				Functional	subset of	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-08	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	10	
ISM-1030	N/A	A NIDS or NIPS is located immediately inside the outermost firewall for gateways and configured to generate event logs and alerts for network traffic that contravenes any rule in a firewall ruleset.				Functional	equal	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-08	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	10	
ISM-1034	N/A	A HIPS is implemented on critical servers and high-value servers.				Functional	equal	Host Intrusion Detection and Prevention Systems (HIDS / HIPS)	END-07	Mechanisms exist to utilize Host-based Intrusion Detection / Prevention Systems (HIDS / HIPS), or similar technologies, to monitor for and protect against anomalous host activity, including lateral movement across the network.	10	
ISM-1036	N/A	Fax machines and MFDs are located in areas where their use can be observed.				Functional	intersects with	Multi-Function Devices (MFD)	AST-23	Mechanisms exist to securely configure Multi-Function Devices (MFD) according to industry-recognized secure practices for the type of device.	5	
ISM-1036	N/A	Fax machines and MFDs are located in areas where their use can be observed.				Functional	intersects with	Access Control for Output Devices	PES-12.2	Physical security mechanisms exist to restrict access to printers and other system output devices to prevent unauthorized individuals from obtaining the output.	5	
ISM-1037	N/A	Gateways undergo testing following configuration changes, and at regular intervals no more than six months apart, to validate they conform to expected security configurations.				Functional	subset of	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	10	
ISM-1053	N/A	Servers, network devices and cryptographic equipment are secured in server rooms or communications rooms that meet the requirements for a security zone suitable for their classification.				Functional	subset of	Access To Information Systems	PES-03.4	Physical access control mechanisms exist to enforce physical access to critical information systems or sensitive/regulated data, in addition to the physical access controls for the facility.	10	
ISM-1055	N/A	LAN Manager and NT LAN Manager authentication methods are disabled.				Functional	subset of	Replay-Resistant Authentication	IAC-02.2	Automated mechanisms exist to employ replay-resistant authentication.	10	
ISM-1059	N/A	All data stored on media is encrypted.				Functional	subset of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
ISM-1059	N/A	All data stored on media is encrypted.				Functional	intersects with	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive / regulated data is formally trained in data handling requirements.	5	
ISM-1065	N/A	The host-protected area and device configuration overlay table are reset prior to the sanitisation of non-volatile magnetic hard drives.				Functional	subset of	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	10	
ISM-1067	N/A	The ATA secure erase command is used, in addition to block overwriting software, to ensure the growth defects table of non-volatile magnetic hard drives is overwritten.				Functional	subset of	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	10	
ISM-1071	N/A	Each system has a designated system owner.				Functional	equal	Asset Ownership Assignment	AST-03	Mechanisms exist to maintain a current list of approved technologies (hardware and software).	10	
ISM-1073	N/A	An organisation's systems, applications and data are not accessed or administered by a service provider unless a contractual arrangement exists between the organisation and the service provider to do so.				Functional	subset of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
ISM-1074	N/A	Keys or equivalent access mechanisms to server rooms, communications rooms, security containers and secure rooms are appropriately controlled.				Functional	subset of	Access To Information Systems	PES-03.4	Physical access control mechanisms exist to enforce physical access to critical information systems or sensitive/regulated data, in addition to the physical access controls for the facility.	10	
ISM-1075	N/A	The sender of a fax message makes arrangements for the receiver to collect the fax message as soon as possible after it is sent and for the receiver to notify the sender if the fax message does not arrive in an agreed amount of time.				Functional	subset of	Use of Communications Technology	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	Essential 8 ML1	Essential 8 ML1	Essential 8 ML1	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
ISM-1076	N/A	Televisions and computer monitors with minor burn-in or image persistence are sanitised by displaying a solid white image on the screen for an extended period of time.				Functional	subset of	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	10	
ISM-1078	N/A	A telephone system usage policy is developed, implemented and maintained.				Functional	subset of	Use of Communications Technology	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously.	10	
ISM-1079	N/A	ASD's approval is sought before undertaking any maintenance or repairs to high assurance IT equipment.				Functional	subset of	Controlled Maintenance	MNT-02	Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the system, application or service.	10	
ISM-1080	N/A	An ASD-Approved Cryptographic Algorithm (AACA) or high assurance cryptographic algorithm is used when encrypting media.				Functional	subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
ISM-1080	N/A	An ASD-Approved Cryptographic Algorithm (AACA) or high assurance cryptographic algorithm is used when encrypting media.				Functional	intersects with	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
ISM-1080	N/A	An ASD-Approved Cryptographic Algorithm (AACA) or high assurance cryptographic algorithm is used when encrypting media.				Functional	intersects with	Database Encryption	CRY-05.3	Mechanisms exist to ensure that database servers utilize encryption to protect the confidentiality of the data within the databases.	5	
ISM-1082	N/A	A mobile device usage policy is developed, implemented and maintained.				Functional	subset of	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	10	
ISM-1083	N/A	Personnel are advised of the sensitivity or classification permitted for voice and data communications when using mobile devices.				Functional	subset of	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	10	
ISM-1084	N/A	If unable to carry or store mobile devices in a secured state, they are physically transferred in a security briefcase or an approved multi-use satchel, pouch or transit bag.				Functional	subset of	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	10	
ISM-1085	N/A	Mobile devices encrypt all sensitive or classified data communicated over public network infrastructure.				Functional	subset of	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	10	
ISM-1088	N/A	Personnel report the potential compromise of mobile devices, removable media or credentials to their organisation as soon as possible, especially if they: - provide credentials to foreign government officials - decrypt mobile devices for foreign government officials - have mobile devices taken out of sight by foreign government officials - have mobile devices or removable media stolen, including if later returned - lose mobile devices or removable media, including if later found - observe unusual behaviour of mobile devices.				Functional	intersects with	Travel-Only Devices	AST-24	Mechanisms exist to issue personnel travelling overseas with temporary, loaner or "travel-only" end user technology (e.g., laptops and mobile devices) when travelling to authoritarian countries with a higher-than average risk for Intellectual Property (IP) theft or espionage against individuals and private companies.	5	
ISM-1088	N/A	Personnel report the potential compromise of mobile devices, removable media or credentials to their organisation as soon as possible, especially if they: - provide credentials to foreign government officials - decrypt mobile devices for foreign government officials - have mobile devices taken out of sight by foreign government officials - have mobile devices or removable media stolen, including if later returned - lose mobile devices or removable media, including if later found - observe unusual behaviour of mobile devices.				Functional	intersects with	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.	5	
ISM-1089	N/A	Protective marking tools do not allow users replying to or forwarding emails to select protective markings lower than previously used.				Functional	subset of	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	10	
ISM-1091	N/A	Keying material is changed when compromised or suspected of being compromised.				Functional	subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
ISM-1091	N/A	Keying material is changed when compromised or suspected of being compromised.				Functional	intersects with	Monitoring for Indicators of Compromise (IOC)	MON-11.3	Automated mechanisms exist to identify and alert on Indicators of Compromise (IoC).	5	
ISM-1092	N/A	Separate fax machines or MFDs are used for sending sensitive or classified fax messages and all other fax messages.				Functional	subset of	Use of Communications Technology	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously.	10	
ISM-1095	N/A	Wall outlet boxes denote the systems, cable identifiers and wall outlet box identifier.				Functional	subset of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
ISM-1096	N/A	Cables are labelled at each end with sufficient source and destination details to enable the physical identification and inspection of the cable.				Functional	subset of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
ISM-1098	N/A	SECRET cables are terminated in an individual cabinet; or for small systems, a cabinet with a division plate between any SECRET cables and non-SECRET cables.				Functional	subset of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
ISM-1100	N/A	TOP SECRET cables are terminated in an individual TOP SECRET cabinet.				Functional	subset of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
ISM-1101	N/A	In TOP SECRET areas, cable reticulation systems leading into cabinets in server rooms or communications rooms are terminated as close as possible to the cabinet.				Functional	subset of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
ISM-1102	N/A	Cable reticulation systems leading into cabinets are terminated as close as possible to the cabinet.				Functional	subset of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
ISM-1103	N/A	In TOP SECRET areas, cable reticulation systems leading into cabinets not in server rooms or communications rooms are terminated at the boundary of the cabinet.				Functional	subset of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
ISM-1105	N/A	SECRET and TOP SECRET wall outlet boxes contain exclusively SECRET or TOP SECRET cables.				Functional	subset of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
ISM-1107	N/A	OFFICIAL: Sensitive and PROTECTED wall outlet boxes are coloured neither salmon pink nor red.				Functional	intersects with	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
ISM-1107	N/A	OFFICIAL: Sensitive and PROTECTED wall outlet boxes are coloured neither salmon pink nor red.				Functional	intersects with	Component Marking	PES-16	Physical security mechanisms exist to mark system hardware components indicating the impact or classification level of the information permitted to be processed, stored or transmitted by the hardware component.	5	
ISM-1109	N/A	Wall outlet box covers are clear plastic.				Functional	subset of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
ISM-1111	N/A	Fibre-optic cables are used for cabling infrastructure instead of copper cables.				Functional	subset of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
ISM-1112	N/A	Cables are inspectable at a minimum of five-metre intervals.				Functional	subset of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
ISM-1114	N/A	Cable bundles or conduits sharing a common cable reticulation system have a dividing partition or visible gap between each cable bundle and conduit.				Functional	subset of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
ISM-1115	N/A	Cables from cable trays to wall outlet boxes are run in flexible or plastic conduit.				Functional	subset of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
ISM-1116	N/A	A visible gap exists between TOP SECRET cabinets and non-TOP SECRET cabinets.				Functional	subset of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
ISM-1119	N/A	Cables in TOP SECRET areas are fully inspectable for their entire length.				Functional	subset of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
ISM-1122	N/A	Where wall penetrations exit a TOP SECRET area into a lower classified area, TOP SECRET cables are encased in conduit with all gaps between the TOP SECRET conduit and the wall filled with an appropriate sealing compound.				Functional	subset of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
ISM-1123	N/A	A power distribution board with a feed from an Uninterruptible Power Supply is used to power all TOP SECRET IT equipment.				Functional	subset of	Emergency Power	PES-07.3	Facility security mechanisms exist to supply alternate power, capable of maintaining minimally-required operational capability, in the event of an extended loss of the primary power source.	10	
ISM-1130	N/A	In shared facilities, cables are run in an enclosed cable reticulation system.				Functional	subset of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
ISM-1133	N/A	In shared facilities, TOP SECRET cables are not run in party walls.				Functional	subset of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
ISM-1137	N/A	System owners deploying SECRET or TOP SECRET systems within fixed facilities contact ASD for an emanation security threat assessment.				Functional	subset of	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; and/or (11) Artificial Intelligence and Autonomous Technologies (AAT).	10	
ISM-1139	N/A	Only the latest version of TLS is used for TLS connections.				Functional	subset of	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	10	
ISM-1143	N/A	Patch management processes, and supporting patch management procedures, are developed, implemented and maintained.				Functional	subset of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
ISM-1143	N/A	Patch management processes, and supporting patch management procedures, are developed, implemented and maintained.				Functional	intersects with	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	5	
ISM-1145	N/A	Privacy filters are applied to the screens of SECRET and TOP SECRET mobile devices.				Functional	subset of	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	Essential 8 ML1	Essential 8 ML1	Essential 8 ML1	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
ISM-1146	N/A	Personnel are advised to maintain separate work and personal accounts for online services.				Functional	subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
ISM-1146	N/A	Personnel are advised to maintain separate work and personal accounts for online services.				Functional	subset of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
ISM-1146	N/A	Personnel are advised to maintain separate work and personal accounts for online services.				Functional	intersects with	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	
ISM-1146	N/A	Personnel are advised to maintain separate work and personal accounts for online services.				Functional	intersects with	Cybersecurity & Data Privacy Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	
ISM-1146	N/A	Personnel are advised to maintain separate work and personal accounts for online services.				Functional	intersects with	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
ISM-1151	N/A	SPF is used to verify the authenticity of incoming emails.				Functional	intersects with	Domain Name Service (DNS) Resolution	NET-10	Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.	5	
ISM-1151	N/A	SPF is used to verify the authenticity of incoming emails.				Functional	intersects with	Sender Policy Framework (SPF)	NET-10.3	Mechanisms exist to validate the legitimacy of email communications through configuring a Domain Naming Service (DNS) Sender Policy Framework (SPF) record to specify the IP addresses and/or hostnames that are authorized to send email from the specified domain.	5	
ISM-1151	N/A	SPF is used to verify the authenticity of incoming emails.				Functional	intersects with	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
ISM-1157	N/A	Evaluated diodes are used for controlling the data flow of unidirectional gateways between networks.				Functional	subset of	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	10	
ISM-1158	N/A	Evaluated diodes used for controlling the data flow of unidirectional gateways between SECRET or TOP SECRET networks and any other networks complete a high assurance evaluation.				Functional	subset of	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	10	
ISM-1160	N/A	If using degaussers to destroy media, degaussers evaluated by the United States' National Security Agency are used.				Functional	subset of	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	10	
ISM-1163	N/A	Systems have a continuous monitoring plan that includes: - Conducting vulnerability scans for systems at least fortnightly - Conducting vulnerability assessments and penetration tests for systems prior to deployment, including prior to deployment of significant changes, and at least annually thereafter - Analysing identified vulnerabilities to determine their potential impact - Implementing mitigations based on risk, effectiveness and cost.				Functional	subset of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
ISM-1163	N/A	Systems have a continuous monitoring plan that includes: - Conducting vulnerability scans for systems at least fortnightly - Conducting vulnerability assessments and penetration tests for systems prior to deployment, including prior to deployment of significant changes, and at least annually thereafter - Analysing identified vulnerabilities to determine their potential impact - Implementing mitigations based on risk, effectiveness and cost.				Functional	subset of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
ISM-1163	N/A	Systems have a continuous monitoring plan that includes: - Conducting vulnerability scans for systems at least fortnightly - Conducting vulnerability assessments and penetration tests for systems prior to deployment, including prior to deployment of significant changes, and at least annually thereafter - Analysing identified vulnerabilities to determine their potential impact - Implementing mitigations based on risk, effectiveness and cost.				Functional	intersects with	Vulnerability Ranking	VPM-03	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	5	
ISM-1163	N/A	Systems have a continuous monitoring plan that includes: - Conducting vulnerability scans for systems at least fortnightly - Conducting vulnerability assessments and penetration tests for systems prior to deployment, including prior to deployment of significant changes, and at least annually thereafter - Analysing identified vulnerabilities to determine their potential impact - Implementing mitigations based on risk, effectiveness and cost.				Functional	intersects with	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
ISM-1163	N/A	Systems have a continuous monitoring plan that includes: - Conducting vulnerability scans for systems at least fortnightly - Conducting vulnerability assessments and penetration tests for systems prior to deployment, including prior to deployment of significant changes, and at least annually thereafter - Analysing identified vulnerabilities to determine their potential impact - Implementing mitigations based on risk, effectiveness and cost.				Functional	intersects with	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on systems and web applications.	5	
ISM-1164	N/A	In shared facilities, conduits or the front covers of ducts, cable trays in floors and ceilings, and associated fittings are clear plastic.				Functional	subset of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
ISM-1171	N/A	Attempts to access websites through their IP addresses instead of their domain names are blocked by web content filters.				Functional	subset of	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	10	
ISM-1173	N/A	Multi-factor authentication is used to authenticate privileged users of systems.		ML2	ML3	Functional	equal	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	10	Essential Eight: ML2, ML3
ISM-1175	N/A	Privileged accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services.	ML1	ML2	ML3	Functional	subset of	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.	10	Essential Eight: ML1, ML2, ML3
ISM-1178	N/A	Network documentation provided to a third party, or published in public tender documentation, only contains details necessary for other parties to undertake contractual services.				Functional	subset of	Security of Assets & Media	AST-05	Mechanisms exist to maintain strict control over the internal or external distribution of any kind of sensitive/regulated media.	10	
ISM-1181	N/A	Networks are segregated into multiple network zones according to the criticality of servers, services and data.				Functional	equal	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	10	
ISM-1182	N/A	Network access controls are implemented to limit the flow of network traffic within and between network segments to only that required for business purposes.				Functional	equal	Network Access Control (NAC)	AST-02.5	Mechanisms exist to maintain a current list of approved technologies (hardware and software).	10	
ISM-1183	N/A	A hard fail SPF record is used when specifying authorised email servers (or lack thereof) for an organisation's domains (including subdomains).				Functional	intersects with	Domain Name Service (DNS) Resolution	NET-10	Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.	5	
ISM-1183	N/A	A hard fail SPF record is used when specifying authorised email servers (or lack thereof) for an organisation's domains (including subdomains).				Functional	intersects with	Sender Policy Framework (SPF)	NET-10.3	Mechanisms exist to validate the legitimacy of email communications through configuring a Domain Naming Service (DNS) Sender Policy Framework (SPF) record to specify the IP addresses and/or hostnames that are authorized to send email from the specified domain.	5	
ISM-1183	N/A	A hard fail SPF record is used when specifying authorised email servers (or lack thereof) for an organisation's domains (including subdomains).				Functional	intersects with	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
ISM-1186	N/A	IPv6 capable network security appliances are used on IPv6 and dual-stack networks.				Functional	subset of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
ISM-1187	N/A	When manually exporting data from systems, the data is checked for unsuitable protective markings.				Functional	subset of	Information Sharing	DCH-14	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	10	
ISM-1192	N/A	Gateways inspect and filter data flows at the transport and above network layers.				Functional	subset of	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	10	
ISM-1195	N/A	Mobile Device Management solutions that have completed a Common Criteria evaluation against the Protection Profile for Mobile Device Management, version 4.0 or later, are used to enforce mobile device management policy.				Functional	subset of	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	10	
ISM-1196	N/A	OFFICIAL: Sensitive and PROTECTED mobile devices are configured to remain undiscoverable to other Bluetooth devices except during Bluetooth pairing.				Functional	intersects with	Use of Communications Technology	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously.	5	
ISM-1196	N/A	OFFICIAL: Sensitive and PROTECTED mobile devices are configured to remain undiscoverable to other Bluetooth devices except during Bluetooth pairing.				Functional	intersects with	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
ISM-1198	N/A	Bluetooth pairing for OFFICIAL: Sensitive and PROTECTED mobile devices is performed in a manner such that connections are only made between intended Bluetooth devices.				Functional	intersects with	Use of Communications Technology	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously.	5	
ISM-1198	N/A	Bluetooth pairing for OFFICIAL: Sensitive and PROTECTED mobile devices is performed in a manner such that connections are only made between intended Bluetooth devices.				Functional	intersects with	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
ISM-1199	N/A	Bluetooth pairings for OFFICIAL: Sensitive and PROTECTED mobile devices are removed when there is no longer a requirement for their use.				Functional	intersects with	Bluetooth & Wireless Devices	AST-14.1	Mechanisms exist to prevent the usage of Bluetooth and wireless devices (e.g., Near Field Communications (NFC)) in sensitive areas or unless used in a Radio Frequency (RF)-screened building.	5	
ISM-1199	N/A	Bluetooth pairings for OFFICIAL: Sensitive and PROTECTED mobile devices are removed when there is no longer a requirement for their use.				Functional	intersects with	Use of Communications Technology	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously.	5	
ISM-1199	N/A	Bluetooth pairings for OFFICIAL: Sensitive and PROTECTED mobile devices are removed when there is no longer a requirement for their use.				Functional	intersects with	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
ISM-1200	N/A	Bluetooth pairing for OFFICIAL: Sensitive and PROTECTED mobile devices is performed using Secure Connections, preferably with Numeric Comparison if supported.				Functional	intersects with	Bluetooth & Wireless Devices	AST-14.1	Mechanisms exist to prevent the usage of Bluetooth and wireless devices (e.g., Near Field Communications (NFC)) in sensitive areas or unless used in a Radio Frequency (RF)-screened building.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	Essential 8 ML1	Essential 8 ML1	Essential 8 ML1	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
ISM-1200	N/A	Bluetooth pairing for OFFICIAL: Sensitive and PROTECTED mobile devices is performed using Secure Connections, preferably with Numeric Comparison if supported.				Functional	intersects with	Use of Communications Technology	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously.	5	
ISM-1200	N/A	Bluetooth pairing for OFFICIAL: Sensitive and PROTECTED mobile devices is performed using Secure Connections, preferably with Numeric Comparison if supported.				Functional	intersects with	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
ISM-1211	N/A	System administrators document requirements for administrative activities, consider potential security impacts, obtain any necessary approvals, notify users of any disruptions or outages, and maintain system and security documentation.				Functional	subset of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
ISM-1211	N/A	System administrators document requirements for administrative activities, consider potential security impacts, obtain any necessary approvals, notify users of any disruptions or outages, and maintain system and security documentation.				Functional	intersects with	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
ISM-1213	N/A	Following intrusion remediation activities, full network traffic is captured for at least seven days and analysed to determine whether malicious actors have been successfully removed from the system.				Functional	intersects with	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity & data privacy incidents to reduce the likelihood or impact of future incidents.	5	
ISM-1213	N/A	Following intrusion remediation activities, full network traffic is captured for at least seven days and analysed to determine whether malicious actors have been successfully removed from the system.				Functional	intersects with	Event Log Retention	MON-10	Mechanisms exist to retain event logs for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	5	
ISM-1216	N/A	SECRET and TOP SECRET cables with non-conformant cable colouring are banded with the appropriate colour and labelled at inspection points.				Functional	intersects with	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
ISM-1216	N/A	SECRET and TOP SECRET cables with non-conformant cable colouring are banded with the appropriate colour and labelled at inspection points.				Functional	intersects with	Component Marking	PES-16	Physical security mechanisms exist to mark system hardware components indicating the impact or classification level of the information permitted to be processed, stored or transmitted by the hardware component.	5	
ISM-1217	N/A	Labels and markings indicating the owner, sensitivity, classification or any other marking that can associate IT equipment with its prior use are removed prior to its disposal.				Functional	intersects with	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
ISM-1217	N/A	Labels and markings indicating the owner, sensitivity, classification or any other marking that can associate IT equipment with its prior use are removed prior to its disposal.				Functional	intersects with	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
ISM-1217	N/A	Labels and markings indicating the owner, sensitivity, classification or any other marking that can associate IT equipment with its prior use are removed prior to its disposal.				Functional	intersects with	Component Marking	PES-16	Physical security mechanisms exist to mark system hardware components indicating the impact or classification level of the information permitted to be processed, stored or transmitted by the hardware component.	5	
ISM-1218	N/A	IT equipment, including associated media, that is located overseas and has processed, stored or communicated AUSTEO or AGAO data, is sanitised in situ.				Functional	intersects with	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
ISM-1218	N/A	IT equipment, including associated media, that is located overseas and has processed, stored or communicated AUSTEO or AGAO data, is sanitised in situ.				Functional	intersects with	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
ISM-1219	N/A	MFD print drums and image transfer rollers are inspected and destroyed if there is remnant toner which cannot be removed or a print is visible on the image transfer roller.				Functional	subset of	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	10	
ISM-1220	N/A	Printer and MFD platens are inspected and destroyed if any text or images are retained on the platen.				Functional	subset of	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	10	
ISM-1221	N/A	Printers and MFDs are checked to ensure no pages are trapped in the paper path due to a paper jam.				Functional	subset of	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	10	
ISM-1222	N/A	Televisions and computer monitors that cannot be sanitised are destroyed.				Functional	subset of	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	10	
ISM-1223	N/A	Memory in network devices is sanitised using the following processes, in order of preference: - following device-specific guidance provided in evaluation documentation - following vendor sanitisation guidance - loading a dummy configuration file, performing a factory reset and then reinstalling firmware.				Functional	subset of	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	10	
ISM-1225	N/A	The paper tray of the fax machine is removed, and a fax message with a minimum length of four pages is transmitted, before the paper tray is re-installed to allow a fax summary page to be printed.				Functional	subset of	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	10	
ISM-1226	N/A	Fax machines are checked to ensure no pages are trapped in the paper path due to a paper jam.				Functional	subset of	Maintenance Operations	MNT-01	Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise.	10	
ISM-1227	N/A	Credentials set for user accounts are randomly generated.				Functional	subset of	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	10	
ISM-1228	N/A	Cyber security events are analysed in a timely manner to identify cyber security incidents.		ML2	ML3	Functional	intersects with	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	Essential Eight: ML2, ML3
ISM-1228	N/A	Cyber security events are analysed in a timely manner to identify cyber security incidents.		ML2	ML3	Functional	intersects with	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	5	Essential Eight: ML2, ML3
ISM-1228	N/A	Cyber security events are analysed in a timely manner to identify cyber security incidents.		ML2	ML3	Functional	intersects with	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.	5	Essential Eight: ML2, ML3
ISM-1234	N/A	Email content filtering is implemented to filter potentially harmful content in email bodies and attachments.				Functional	subset of	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	10	
ISM-1235	N/A	Add-ons, extensions and plug-ins for office productivity suites, web browsers, email clients, PDF software and security products are restricted 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.	5	
ISM-1235	N/A	Add-ons, extensions and plug-ins for office productivity suites, web browsers, email clients, PDF software and security products are restricted to an organisation-approved set.				Functional	intersects with	Unsupported Internet Browsers & Email Clients	CFG-04.2	Mechanisms exist to allow only approved Internet browsers and email clients to run on systems.	5	
ISM-1236	N/A	Malicious domain names, dynamic domain names and domain names that can be registered anonymously for free are blocked by web content filters.				Functional	subset of	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	10	
ISM-1237	N/A	Web content filtering is applied to outbound web traffic where appropriate.				Functional	intersects with	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
ISM-1237	N/A	Web content filtering is applied to outbound web traffic where appropriate.				Functional	intersects with	Route Internal Traffic to Proxy Servers	NET-18.1	Mechanisms exist to route internal communications traffic to external networks through organization-approved proxy servers at managed interfaces.	5	
ISM-1238	N/A	Threat modelling is used in support of application development.				Functional	equal	Threat Modeling	TDA-06.2	Mechanisms exist to perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.	10	
ISM-1239	N/A	Robust web application frameworks are used in the development of web applications.				Functional	intersects with	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5	
ISM-1239	N/A	Robust web application frameworks are used in the development of web applications.				Functional	intersects with	Web Security Standard	WEB-07	Mechanisms exist to ensure the Open Web Application Security Project (OWASP) Application Security Verification Standard is incorporated into the organization's Secure Systems Development Lifecycle (SSDLC) process.	5	
ISM-1239	N/A	Robust web application frameworks are used in the development of web applications.				Functional	intersects with	Web Application Framework	WEB-08	Mechanisms exist to ensure a robust Web Application Framework is used to aid in the development of secure web applications, including web services, web resources and web APIs.	5	
ISM-1240	N/A	Validation or sanitisation is performed on all input handled by web applications.				Functional	equal	Validation & Sanitization	WEB-09	Mechanisms exist to ensure all input handled by a web application is validated and/or sanitized.	10	
ISM-1241	N/A	Output encoding is performed on all output produced by web applications.				Functional	equal	Output Encoding	WEB-11	Mechanisms exist to ensure output encoding is performed on all content produced by a web application to reduce the likelihood of cross-site scripting and other injection attacks.	10	
ISM-1243	N/A	A database register is developed, implemented, maintained and verified on a regular basis.				Functional	subset of	Database Administrative Processes	AST-28	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	10	
ISM-1245	N/A	All temporary installation files and logs created during server application installation processes are removed after server applications have been installed.				Functional	subset of	Database Management System (DBMS)	AST-28.1	Mechanisms exist to implement and maintain Database Management Systems (DBMSs), where applicable.	10	
ISM-1246	N/A	Server applications are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.				Functional	subset of	Database Management System (DBMS)	AST-28.1	Mechanisms exist to implement and maintain Database Management Systems (DBMSs), where applicable.	10	
ISM-1247	N/A	Unneeded accounts, components, services and functionality of server applications are disabled or removed.				Functional	subset of	Database Management System (DBMS)	AST-28.1	Mechanisms exist to implement and maintain Database Management Systems (DBMSs), where applicable.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	Essential 8 ML1	Essential 8 ML1	Essential 8 ML1	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
ISM-1249	N/A	Server applications are configured to run as a separate account with the minimum privileges needed to perform their functions.				Functional	subset of	Database Management System (DBMS)	AST-28.1	Mechanisms exist to implement and maintain Database Management Systems (DBMSs), where applicable.	10	
ISM-1250	N/A	The accounts under which server applications run have limited access to their underlying server's file system.				Functional	subset of	Database Management System (DBMS)	AST-28.1	Mechanisms exist to implement and maintain Database Management Systems (DBMSs), where applicable.	10	
ISM-1255	N/A	Database users' ability to access, insert, modify and remove database contents is restricted based on their work duties.				Functional	subset of	Database Administrative Processes	AST-28	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	10	
ISM-1256	N/A	File-based access controls are applied to database files.				Functional	subset of	Database Administrative Processes	AST-28	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	10	
ISM-1260	N/A	Default accounts or credentials for server applications, including for any pre-configured accounts, are changed.				Functional	subset of	Database Management System (DBMS)	AST-28.1	Mechanisms exist to implement and maintain Database Management Systems (DBMSs), where applicable.	10	
ISM-1263	N/A	Unique privileged accounts are used for administering individual server applications.				Functional	subset of	Database Management System (DBMS)	AST-28.1	Mechanisms exist to implement and maintain Database Management Systems (DBMSs), where applicable.	10	
ISM-1268	N/A	The need-to-know principle is enforced for database contents through the application of minimum privileges, database views and database roles.				Functional	subset of	Database Administrative Processes	AST-28	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	10	
ISM-1269	N/A	Database servers and web servers are functionally separated.				Functional	intersects with	Database Administrative Processes	AST-28	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	5	
ISM-1269	N/A	Database servers and web servers are functionally separated.				Functional	intersects with	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	5	
ISM-1269	N/A	Database servers and web servers are functionally separated.				Functional	intersects with	Microsegmentation	NET-06.6	Automated mechanisms exist to enable microsegmentation, either physically or virtually, to divide the network according to application and data workflows communications needs.	5	
ISM-1270	N/A	Database servers are placed on a different network segment to user workstations.				Functional	intersects with	Database Administrative Processes	AST-28	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	5	
ISM-1270	N/A	Database servers are placed on a different network segment to user workstations.				Functional	intersects with	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	5	
ISM-1270	N/A	Database servers are placed on a different network segment to user workstations.				Functional	intersects with	Microsegmentation	NET-06.6	Automated mechanisms exist to enable microsegmentation, either physically or virtually, to divide the network according to application and data workflows communications needs.	5	
ISM-1271	N/A	Network access controls are implemented to restrict database server communications to strictly defined network resources, such as web servers, application servers and storage area networks.				Functional	intersects with	Mechanisms exist to prevent "side channel attacks" when using a Content Delivery Network (CDN) by restricting access to the origin server's IP address to the CDN and an authorized management network.	AST-28	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	5	
ISM-1271	N/A	Network access controls are implemented to restrict database server communications to strictly defined network resources, such as web servers, application servers and storage area networks.				Functional	intersects with	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	5	
ISM-1271	N/A	Network access controls are implemented to restrict database server communications to strictly defined network resources, such as web servers, application servers and storage area networks.				Functional	intersects with	Microsegmentation	NET-06.6	Automated mechanisms exist to enable microsegmentation, either physically or virtually, to divide the network according to application and data workflows communications needs.	5	
ISM-1272	N/A	If only local access to a database is required, networking functionality of database management system software is disabled or directed to listen solely to the localhost interface.				Functional	subset of	Database Administrative Processes	AST-28	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	10	
ISM-1273	N/A	Development and testing environments do not use the same database servers as production environments.				Functional	intersects with	Database Administrative Processes	AST-28	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	5	
ISM-1273	N/A	Development and testing environments do not use the same database servers as production environments.				Functional	intersects with	Separation of Development, Testing and Operational Environments	TDA-08	Mechanisms exist to manage separate development, testing and operational environments to reduce the risks of unauthorized access or changes to the operational environment and to ensure no impact to production systems.	5	
ISM-1274	N/A	Database contents from production environments are not used in development or testing environments unless the environment is secured to the same level as the production environment.				Functional	intersects with	Database Administrative Processes	AST-28	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	5	
ISM-1274	N/A	Database contents from production environments are not used in development or testing environments unless the environment is secured to the same level as the production environment.				Functional	intersects with	Separation of Development, Testing and Operational Environments	TDA-08	Mechanisms exist to manage separate development, testing and operational environments to reduce the risks of unauthorized access or changes to the operational environment and to ensure no impact to production systems.	5	
ISM-1275	N/A	All queries to databases from web applications are filtered for legitimate content and correct syntax.				Functional	intersects with	Database Administrative Processes	AST-28	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	5	
ISM-1275	N/A	All queries to databases from web applications are filtered for legitimate content and correct syntax.				Functional	intersects with	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
ISM-1276	N/A	Parameterised queries or stored procedures, instead of dynamically generated queries, are used by web applications for database interactions.				Functional	subset of	Database Administrative Processes	AST-28	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	10	
ISM-1277	N/A	Data communicated between database servers and web servers is encrypted.				Functional	intersects with	Database Administrative Processes	AST-28	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	5	
ISM-1277	N/A	Data communicated between database servers and web servers is encrypted.				Functional	intersects with	Database Encryption	CRY-05.3	Mechanisms exist to ensure that database servers utilize encryption to protect the confidentiality of the data within the databases.	5	
ISM-1278	N/A	Web applications are designed or configured to provide as little error information as possible about the structure of databases.				Functional	subset of	Database Administrative Processes	AST-28	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	10	
ISM-1284	N/A	Files imported or exported via gateways or CDSs undergo content validation.				Functional	intersects with	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
ISM-1284	N/A	Files imported or exported via gateways or CDSs undergo content validation.				Functional	intersects with	Heuristic / Nonsignature-Based Detection	END-04.4	Mechanisms exist to utilize heuristic / nonsignature-based antimalware detection capabilities.	5	
ISM-1284	N/A	Files imported or exported via gateways or CDSs undergo content validation.				Functional	intersects with	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
ISM-1286	N/A	Files imported or exported via gateways or CDSs undergo content conversion.				Functional	intersects with	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
ISM-1286	N/A	Files imported or exported via gateways or CDSs undergo content conversion.				Functional	intersects with	Heuristic / Nonsignature-Based Detection	END-04.4	Mechanisms exist to utilize heuristic / nonsignature-based antimalware detection capabilities.	5	
ISM-1286	N/A	Files imported or exported via gateways or CDSs undergo content conversion.				Functional	intersects with	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
ISM-1287	N/A	Files imported or exported via gateways or CDSs undergo content sanitisation.				Functional	intersects with	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
ISM-1287	N/A	Files imported or exported via gateways or CDSs undergo content sanitisation.				Functional	intersects with	Cross Domain Solution (CDS)	NET-02.3	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	5	
ISM-1287	N/A	Files imported or exported via gateways or CDSs undergo content sanitisation.				Functional	intersects with	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
ISM-1287	N/A	Files imported or exported via gateways or CDSs undergo content sanitisation.				Functional	intersects with	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
ISM-1288	N/A	Files imported or exported via gateways or CDSs undergo antivirus scanning using multiple different scanning engines.				Functional	intersects with	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
ISM-1288	N/A	Files imported or exported via gateways or CDSs undergo antivirus scanning using multiple different scanning engines.				Functional	intersects with	Heuristic / Nonsignature-Based Detection	END-04.4	Mechanisms exist to utilize heuristic / nonsignature-based antimalware detection capabilities.	5	
ISM-1288	N/A	Files imported or exported via gateways or CDSs undergo antivirus scanning using multiple different scanning engines.				Functional	intersects with	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	Essential 8 ML1	Essential 8 ML1	Essential 8 ML1	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
ISM-1289	N/A	Archive files imported or exported via gateways or CDSs are unpacked in order to undergo content filtering checks.				Functional	intersects with	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
ISM-1289	N/A	Archive files imported or exported via gateways or CDSs are unpacked in order to undergo content filtering checks.				Functional	intersects with	Heuristic / Nonsignature-Based Detection	END-04.4	Mechanisms exist to utilize heuristic / nonsignature-based antimalware detection capabilities.	5	
ISM-1289	N/A	Archive files imported or exported via gateways or CDSs are unpacked in order to undergo content filtering checks.				Functional	intersects with	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
ISM-1290	N/A	Archive files are unpacked in a controlled manner to ensure content filter performance or availability is not adversely affected.				Functional	subset of	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	10	
ISM-1293	N/A	Encrypted files imported or exported via gateways or CDSs are decrypted in order to undergo content filtering checks.				Functional	intersects with	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
ISM-1293	N/A	Encrypted files imported or exported via gateways or CDSs are decrypted in order to undergo content filtering checks.				Functional	intersects with	Heuristic / Nonsignature-Based Detection	END-04.4	Mechanisms exist to utilize heuristic / nonsignature-based antimalware detection capabilities.	5	
ISM-1293	N/A	Encrypted files imported or exported via gateways or CDSs are decrypted in order to undergo content filtering checks.				Functional	intersects with	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
ISM-1293	N/A	Encrypted files imported or exported via gateways or CDSs are decrypted in order to undergo content filtering checks.				Functional	intersects with	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited internet sites.	5	
ISM-1294	N/A	Data transfer logs for systems are partially verified at least monthly.				Functional	subset of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
ISM-1294	N/A	Data transfer logs for systems are partially verified at least monthly.				Functional	subset of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
ISM-1296	N/A	Physical security is implemented to protect network devices in public areas from physical damage or unauthorised access.				Functional	subset of	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	10	
ISM-1297	N/A	Legal advice is sought prior to allowing privately-owned mobile devices and desktop computers to access systems or data.				Functional	intersects with	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
ISM-1297	N/A	Legal advice is sought prior to allowing privately-owned mobile devices and desktop computers to access systems or data.				Functional	subset of	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	10	
ISM-1297	N/A	Legal advice is sought prior to allowing privately-owned mobile devices and desktop computers to access systems or data.				Functional	intersects with	Personally-Owned Mobile Devices	MDM-06	Mechanisms exist to restrict the connection of personally-owned, mobile devices to organizational systems and networks.	5	
ISM-1298	N/A	Personnel are advised of privacy and security risks when travelling overseas with mobile devices.				Functional	subset of	Travel-Only Devices	AST-24	Mechanisms exist to issue personnel travelling overseas with temporary, loaner or "travel-only" end user technology (e.g., laptops and mobile devices) when travelling to authoritarian countries with a higher-than average risk for Intellectual Property (IP) theft or espionage against individuals and private companies.	10	
ISM-1299	N/A	Personnel are advised to take the following precautions when using mobile devices: - Never leave mobile devices or removable media unattended, including by placing them in checked-in luggage or leaving them in hotel safes - Never store credentials with mobile devices that they grant access to, such as in laptop computer bags - Never lend mobile devices or removable media to untrusted people, even if briefly - Never allow untrusted people to connect their mobile devices or removable media to your mobile devices, including for charging - Never connect mobile devices to designated charging stations or wall outlet charging ports - Never use gifted or unauthorised peripherals, chargers or removable media with mobile devices - Never use removable media for data transfers or backups that have not been checked for malicious code beforehand - Avoid reuse of removable media once used with other parties' systems or mobile devices - Avoid connecting mobile devices to open or untrusted Wi-Fi networks - Consider disabling any communications capabilities of mobile devices when not in use, such as Wi-Fi, Bluetooth, Near Field Communication and ultra-wideband - Consider periodically rebooting mobile devices - Consider using a VPN connection to encrypt all cellular and wireless communications - Consider using encrypted email or messaging apps for all communications.				Functional	subset of	Travel-Only Devices	AST-24	Mechanisms exist to issue personnel travelling overseas with temporary, loaner or "travel-only" end user technology (e.g., laptops and mobile devices) when travelling to authoritarian countries with a higher-than average risk for Intellectual Property (IP) theft or espionage against individuals and private companies.	10	
ISM-1300	N/A	Upon returning from travelling overseas with mobile devices, personnel take the following actions: - Sanitise and reset mobile devices, including all removable media - Decommission any credentials that left their possession during their travel - Report if significant doubt exists as to the integrity of any mobile devices or removable media.				Functional	intersects with	Travel-Only Devices	AST-24	Mechanisms exist to issue personnel travelling overseas with temporary, loaner or "travel-only" end user technology (e.g., laptops and mobile devices) when travelling to authoritarian countries with a higher-than average risk for Intellectual Property (IP) theft or espionage against individuals and private companies.	5	
ISM-1300	N/A	Upon returning from travelling overseas with mobile devices, personnel take the following actions: - Sanitise and reset mobile devices, including all removable media - Decommission any credentials that left their possession during their travel - Report if significant doubt exists as to the integrity of any mobile devices or removable media.				Functional	intersects with	Re-Imaging Devices After Travel	AST-25	Mechanisms exist to re-image end user technology (e.g., laptops and mobile devices) when returning from overseas travel to an authoritarian country with a higher-than average risk for Intellectual Property (IP) theft or espionage against individuals and private companies.	5	
ISM-1300	N/A	Upon returning from travelling overseas with mobile devices, personnel take the following actions: - Sanitise and reset mobile devices, including all removable media - Decommission any credentials that left their possession during their travel - Report if significant doubt exists as to the integrity of any mobile devices or removable media.				Functional	intersects with	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
ISM-1304	N/A	Default accounts or credentials for network devices including for any pre-configured accounts, are changed.				Functional	subset of	Default Authenticators	IAC-10.8	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	10	
ISM-1311	N/A	SNMP version 1 and SNMP version 2 are not used on networks.				Functional	subset of	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	10	
ISM-1312	N/A	All default SNMP community strings on network devices are changed and write access is disabled.				Functional	subset of	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	10	
ISM-1314	N/A	All wireless devices are Wi-Fi Alliance certified.				Functional	intersects with	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	
ISM-1314	N/A	All wireless devices are Wi-Fi Alliance certified.				Functional	intersects with	Limit Network Connections	NET-03.1	Mechanisms exist to limit the number of concurrent external network connections to its systems.	5	
ISM-1314	N/A	All wireless devices are Wi-Fi Alliance certified.				Functional	intersects with	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
ISM-1315	N/A	The administrative interface on wireless access points is disabled for wireless network connections.				Functional	subset of	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	10	
ISM-1316	N/A	Default SSIDs of wireless access points are changed.				Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
ISM-1316	N/A	Default SSIDs of wireless access points are changed.				Functional	intersects with	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
ISM-1317	N/A	SSIDs of non-public wireless networks are not readily associated with an organisation, the location of their premises or the functionality of wireless networks.				Functional	subset of	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	10	
ISM-1318	N/A	SSID broadcasting is not disabled on wireless access points.				Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
ISM-1318	N/A	SSID broadcasting is not disabled on wireless access points.				Functional	intersects with	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
ISM-1319	N/A	Static addressing is not used for assigning IP addresses on wireless networks.				Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
ISM-1319	N/A	Static addressing is not used for assigning IP addresses on wireless networks.				Functional	intersects with	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
ISM-1320	N/A	MAC address filtering is not used to restrict which devices can connect to wireless networks.				Functional	subset of	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	10	
ISM-1321	N/A	802.1X authentication with EAP-TLS, using X.509 certificates, is used for mutual authentication; with all other EAP methods disabled on supplications and authentication servers.				Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
ISM-1321	N/A	802.1X authentication with EAP-TLS, using X.509 certificates, is used for mutual authentication; with all other EAP methods disabled on supplications and authentication servers.				Functional	intersects with	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
ISM-1322	N/A	Evaluated supplicants, authenticators, wireless access points and authentication servers are used in wireless networks.				Functional	subset of	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	10	
ISM-1323	N/A	Certificates are required for devices and users accessing wireless networks.				Functional	subset of	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	10	
ISM-1324	N/A	Certificates are generated using an evaluated certificate authority or hardware security module.				Functional	subset of	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	10	
ISM-1327	N/A	Certificates are protected by logical and physical access controls, encryption, and user authentication.				Functional	subset of	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	Essential 8 ML1	Essential 8 ML1	Essential 8 ML1	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
ISM-1330	N/A	The PMK caching period is not set to greater than 1440 minutes (24 hours).				Functional	subset of	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	10	
ISM-1332	N/A	WPA3-Enterprise 192-bit mode is used to protect the confidentiality and integrity of all wireless network traffic.				Functional	subset of	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	10	
ISM-1334	N/A	Wireless networks implement sufficient frequency separation from other wireless networks.				Functional	subset of	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	10	
ISM-1335	N/A	Wireless access points enable the use of the 802.11w amendment to protect management frames.				Functional	subset of	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	10	
ISM-1338	N/A	Instead of deploying a small number of wireless access points that broadcast on high power, a greater number of wireless access points that use less broadcast power are deployed to achieve the desired footprint for wireless networks.				Functional	subset of	Wireless Boundaries	NET-15.4	Mechanisms exist to confine wireless communications to organization-controlled boundaries.	10	
ISM-1341	N/A	A HIPS is implemented on workstations.				Functional	equal	Host Intrusion Detection and Prevention Systems (HIDS / HIPS)	END-07	Mechanisms exist to utilize Host-based Intrusion Detection / Prevention Systems (HIDS / HIPS), or similar technologies, to monitor for and protect against anomalous host activity, including lateral movement across the network.	10	
ISM-1359	N/A	A removable media usage policy is developed, implemented and maintained.				Functional	subset of	Removable Media Security	DCH-12	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	10	
ISM-1361	N/A	Security Construction and Equipment Committee-approved equipment or ASIO-approved equipment is used when destroying media.				Functional	subset of	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	10	
ISM-1364	N/A	Network devices managing VLANs terminate VLANs belonging to different security domains on separate physical network interfaces.				Functional	subset of	Virtual Local Area Network (VLAN) Separation	NET-06.2	Mechanisms exist to enable Virtual Local Area Networks (VLANs) to limit the ability of devices on a network to directly communicate with other devices on the subnet and limit an attacker's ability to laterally move to compromise neighboring systems.	10	
ISM-1366	N/A	Security updates are applied to mobile devices as soon as they become available.				Functional	intersects with	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
ISM-1366	N/A	Security updates are applied to mobile devices as soon as they become available.				Functional	subset of	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	10	
ISM-1369	N/A	AES-GCM is used for encryption of TLS connections.				Functional	subset of	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	10	
ISM-1370	N/A	Only server-initiated secure renegotiation is used for TLS connections.				Functional	subset of	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	10	
ISM-1372	N/A	DH or ECDH is used for key establishment of TLS connections.				Functional	subset of	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	10	
ISM-1373	N/A	Anonymous DH is not used for TLS connections.				Functional	subset of	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	10	
ISM-1374	N/A	SHA-2-based certificates are used for TLS connections.				Functional	subset of	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	10	
ISM-1375	N/A	SHA-2 is used for the Hash-based Message Authentication Code (HMAC) and pseudorandom function (PRF) for TLS connections.				Functional	subset of	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	10	
ISM-1380	N/A	Privileged users use separate privileged and unprivileged operating environments.	ML1	ML2	ML3	Functional	intersects with	System Administrative Processes	AST-26	Mechanisms exist to develop, implement and govern system administration processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining systems, applications and services.	5	Essential Eight: ML1, ML2, ML3
ISM-1380	N/A	Privileged users use separate privileged and unprivileged operating environments.	ML1	ML2	ML3	Functional	intersects with	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.	5	Essential Eight: ML1, ML2, ML3
ISM-1380	N/A	Privileged users use separate privileged and unprivileged operating environments.	ML1	ML2	ML3	Functional	intersects with	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	Essential Eight: ML1, ML2, ML3
ISM-1385	N/A	Administrative infrastructure is segregated from the wider network and the internet.				Functional	intersects with	System Administrative Processes	AST-26	Mechanisms exist to develop, implement and govern system administration processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining systems, applications and services.	5	
ISM-1385	N/A	Administrative infrastructure is segregated from the wider network and the internet.				Functional	intersects with	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.	5	
ISM-1385	N/A	Administrative infrastructure is segregated from the wider network and the internet.				Functional	intersects with	Cloud Infrastructure Security Subnet	CLD-03	Mechanisms exist to host security-specific technologies in a dedicated subnet.	5	
ISM-1385	N/A	Administrative infrastructure is segregated from the wider network and the internet.				Functional	intersects with	Security Management Subnets	NET-06.1	Mechanisms exist to implement security management subnets to isolate security tools and support components from other internal system components by implementing separate subnetworks with managed interfaces to other components of the system.	5	
ISM-1385	N/A	Administrative infrastructure is segregated from the wider network and the internet.				Functional	intersects with	Segregation From Enterprise Services	NET-06.4	Mechanisms exist to isolate sensitive / regulated data enclaves (secure zones) from corporate-provided IT resources by providing enclave-specific IT services (e.g., directory services, DNS, NTP, ITAM, antimalware, patch management, etc.) to those isolated network segments.	5	
ISM-1386	N/A	Network management traffic can only originate from administrative infrastructure.				Functional	subset of	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	10	
ISM-1387	N/A	Administrative activities are conducted through jump servers.		ML2	ML3	Functional	equal	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	Essential Eight: ML2, ML3
ISM-1389	N/A	Executable files imported via gateways or CDSs are automatically executed in a sandbox to detect any suspicious behaviour.				Functional	intersects with	Detonation Chambers (Sandboxes)	IRO-15	Mechanisms exist to utilize a detonation chamber capability to detect and/or block potentially-malicious files and email attachments.	5	
ISM-1389	N/A	Executable files imported via gateways or CDSs are automatically executed in a sandbox to detect any suspicious behaviour.				Functional	intersects with	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
ISM-1392	N/A	When implementing application control using path rules, only approved users can modify approved files and write to approved folders.				Functional	intersects with	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5	
ISM-1392	N/A	When implementing application control using path rules, only approved users can modify approved files and write to approved folders.				Functional	intersects with	Configuration Enforcement	CFG-06	Automated mechanisms exist to monitor, enforce and report on configurations for endpoint devices.	5	
ISM-1392	N/A	When implementing application control using path rules, only approved users can modify approved files and write to approved folders.				Functional	intersects with	Integrity Assurance & Enforcement (IAE)	CFG-06.1	Automated mechanisms exist to identify unauthorized deviations from an approved baseline and implement automated resiliency actions to remediate the unauthorized change.	5	
ISM-1392	N/A	When implementing application control using path rules, only approved users can modify approved files and write to approved folders.				Functional	intersects with	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
ISM-1395	N/A	Service providers, including any subcontractors, provide an appropriate level of protection for any data entrusted to them or their services.				Functional	subset of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	10	
ISM-1400	N/A	Personnel accessing OFFICIAL: Sensitive or PROTECTED systems or data using privately-owned mobile devices or desktop computers have enforced separation of work data from personal data.				Functional	subset of	Personally-Owned Mobile Devices	MDM-06	Mechanisms exist to restrict the connection of personally-owned, mobile devices to organizational systems and networks.	10	
ISM-1401	N/A	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.	ML1	ML2	ML3	Functional	equal	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	10	Essential Eight: ML1, ML2, ML3
ISM-1402	N/A	Credentials stored on systems are protected by a password manager; a hardware security module; or by salting, hashing and stretching them before storage within a database.				Functional	equal	Protection of Authenticators	IAC-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	10	
ISM-1403	N/A	Accounts, except for break glass accounts, are locked out after a maximum of five failed logon attempts.				Functional	equal	Account Lockout	IAC-22	Mechanisms exist to enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period and automatically locks the account when the maximum number of unsuccessful attempts is exceeded.	10	
ISM-1404	N/A	Unprivileged access to systems and applications is disabled after 45 days of inactivity.				Functional	equal	Disable Inactive Accounts	IAC-15.3	Automated mechanisms exist to disable inactive accounts after an organization-defined time period.	10	
ISM-1405	N/A	A centralised event logging facility is implemented and event logs are sent to the facility as soon as possible after they occur.				Functional	equal	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	10	
ISM-1406	N/A	SOEs are used for workstations and servers.				Functional	subset of	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	10	
ISM-1407	N/A	The latest release, or the previous release, of operating systems are used.			ML3	Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	Essential Eight: ML3
ISM-1407	N/A	The latest release, or the previous release, of operating systems are used.			ML3	Functional	intersects with	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and upgrades.	5	
ISM-1408	N/A	Where supported, 64-bit versions of operating systems are used.				Functional	subset of	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	10	
ISM-1409	N/A	Operating systems are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.				Functional	subset of	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	10	
ISM-1412	N/A	Web browsers are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.		ML2	ML3	Functional	subset of	Unsupported Internet Browsers & Email Clients	CFG-04.2	Mechanisms exist to allow only approved Internet browsers and email clients to run on systems.	10	Essential Eight: ML2, ML3
ISM-1416	N/A	A software firewall is implemented on workstations and servers to restrict inbound and outbound network connections to an organisation-approved set of applications and services.				Functional	equal	Software Firewall	END-05	Mechanisms exist to utilize host-based firewall software, or a similar technology, on all information systems, where technically feasible.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	Essential 8 ML1	Essential 8 ML1	Essential 8 ML1	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
ISM-1417	N/A	Antivirus software is implemented on workstations and servers with: - Signature-based detection functionality enabled and set to a high level - Heuristic-based detection functionality enabled and set to a high level - Reputation rating functionality enabled - Ransomware protection functionality enabled - Detection signatures configured to update on at least a daily basis - Regular scanning configured for all fixed disks and removable media.				Functional	intersects with	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
ISM-1417	N/A	Antivirus software is implemented on workstations and servers with: - Signature-based detection functionality enabled and set to a high level - Heuristic-based detection functionality enabled and set to a high level - Reputation rating functionality enabled - Ransomware protection functionality enabled - Detection signatures configured to update on at least a daily basis - Regular scanning configured for all fixed disks and removable media.				Functional	intersects with	Heuristic / Nonsignature-Based Detection	END-04.4	Mechanisms exist to utilize heuristic / nonsignature-based antimalware detection capabilities.	5	
ISM-1418	N/A	If there is no business requirement for reading from removable media and devices, such functionality is disabled via the use of device access control software or by disabling external communication interfaces.				Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
ISM-1418	N/A	If there is no business requirement for reading from removable media and devices, such functionality is disabled via the use of device access control software or by disabling external communication interfaces.				Functional	intersects with	Host Intrusion Detection and Prevention Systems (HIDS / HIPS)	END-07	Mechanisms exist to utilize Host-based Intrusion Detection / Prevention Systems (HIDS / HIPS), or similar technologies, to monitor for and protect against anomalous host activity, including lateral movement across the network.	5	
ISM-1419	N/A	Development and modification of software only takes place in development environments.				Functional	intersects with	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5	
ISM-1419	N/A	Development and modification of software only takes place in development environments.				Functional	intersects with	Secure Development Environments	TDA-07	Mechanisms exist to maintain a segmented development network to ensure a secure development environment.	5	
ISM-1420	N/A	Data from production environments is not used in a development or testing environment unless the environment is secured to the same level as the production environment.				Functional	equal	Use of Live Data	TDA-10	Mechanisms exist to approve, document and control the use of live data in development and test environments.	10	
ISM-1422	N/A	Unauthorised access to the authoritative source for software is prevented.				Functional	subset of	Access to Program Source Code	TDA-20	Mechanisms exist to limit privileges to change software resident within software libraries.	10	
ISM-1424	N/A	Web applications implement Content-Security-Policy, HSTS and X-Frame-Options via security policy in response headers.				Functional	subset of	Web Browser Security	WEB-12	Mechanisms exist to ensure web applications implement Content-Security-Policy, HSTS and X-Frame-Options response headers to protect both the web application and its users.	10	
ISM-1427	N/A	Gateways perform ingress traffic filtering to detect and prevent IP source address spoofing.				Functional	subset of	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	10	
ISM-1428	N/A	Unless explicitly required, IPv6 tunnelling is disabled on all network devices.				Functional	subset of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
ISM-1429	N/A	IPv6 tunnelling is blocked by network security appliances at externally-connected network boundaries.				Functional	subset of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
ISM-1430	N/A	Dynamically assigned IPv6 addresses are configured with Dynamic Host Configuration Protocol version 6 in a stateful manner with lease data stored in a centralised event logging facility.				Functional	subset of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
ISM-1431	N/A	Denial-of-service attack mitigation strategies are discussed with cloud service providers, specifically: - their capacity to withstand denial-of-service attacks - costs likely to be incurred as a result of denial-of-service attacks - availability monitoring and thresholds for notification of denial-of-service attacks - thresholds for turning off any online services or functionality during denial-of-service attacks - pre-approved actions that can be undertaken during denial-of-service attacks - any arrangements with upstream service providers to block malicious network traffic as far upstream as possible.				Functional	subset of	Denial of Service (DoS) Protection	NET-02.1	Automated mechanisms exist to protect against or limit the effects of denial of service attacks.	10	
ISM-1432	N/A	Domain names for online services are protected via registrar locking and confirming that domain registration details are correct.				Functional	equal	Domain Registrar Security	NET-10.4	Mechanisms exist to lock the domain name registrar to prevent a denial of service caused by unauthorized deletion, transfer or other unauthorized modification of a domain's registration details.	10	
ISM-1436	N/A	Critical online services are segregated from other online services that are more likely to be targeted as part of denial-of- service attacks.				Functional	subset of	Denial of Service (DoS) Protection	NET-02.1	Automated mechanisms exist to protect against or limit the effects of denial of service attacks.	10	
ISM-1437	N/A	Cloud service providers are used for hosting online services.				Functional	subset of	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	10	
ISM-1438	N/A	Where a high availability requirement exists for website hosting, CDNs that cache websites are used.				Functional	subset of	Side Channel Attack Prevention	CLD-12	Mechanisms exist to prevent "side channel attacks" when using a Content Delivery Network (CDN) by restricting access to the origin server's IP address to the CDN and an authorized management network.	10	
ISM-1439	N/A	If using CDNs, disclosing the IP addresses of web servers under an organisation's control (referred to as origin servers) is avoided and access to the origin servers is restricted to the CDNs and authorised management networks.				Functional	subset of	Side Channel Attack Prevention	CLD-12	Mechanisms exist to prevent "side channel attacks" when using a Content Delivery Network (CDN) by restricting access to the origin server's IP address to the CDN and an authorized management network.	10	
ISM-1446	N/A	When using elliptic curve cryptography, a suitable curve from NIST SP 800-186 is used.				Functional	subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
ISM-1448	N/A	When using DH or ECDH for key establishment of TLS connections, the ephemeral variant is used.				Functional	subset of	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	10	
ISM-1449	N/A	SSH private keys are protected with a passphrase or a key encryption key.				Functional	subset of	Public Key Infrastructure (PKI)	CRY-08	Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service provider.	10	
ISM-1450	N/A	Microphones (including headsets and USB handsets) and webcams are not used with non-TOP SECRET workstations in TOP SECRET areas.				Functional	subset of	Microphones & Web Cameras	AST-22	Mechanisms exist to configure assets to prohibit the use of endpoint-based microphones and web cameras in secure areas or where sensitive/regulated information is discussed.	10	
ISM-1451	N/A	Types of data and its ownership is documented in contractual arrangements with service providers.				Functional	intersects with	Adequate Security for Sensitive / Regulated Data In Support of Contracts	IAO-03.2	Mechanisms exist to protect sensitive / regulated data that is collected, developed, received, transmitted, used or stored in support of the performance of a contract.	5	
ISM-1451	N/A	Types of data and its ownership is documented in contractual arrangements with service providers.				Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
ISM-1452	N/A	A supply chain risk assessment is performed for suppliers of applications, IT equipment, OT equipment and services in order to assess the impact to a system's security risk profile				Functional	intersects with	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with systems, system components and services.	5	
ISM-1452	N/A	A supply chain risk assessment is performed for suppliers of applications, IT equipment, OT equipment and services in order to assess the impact to a system's security risk profile				Functional	intersects with	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical systems, components and services using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5	
ISM-1452	N/A	A supply chain risk assessment is performed for suppliers of applications, IT equipment, OT equipment and services in order to assess the impact to a system's security risk profile				Functional	intersects with	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with the services and product supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5	
ISM-1453	N/A	Perfect Forward Secrecy (PFS) is used for TLS connections.				Functional	subset of	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	10	
ISM-1454	N/A	Communications between authenticators and a RADIUS server are encapsulated with an additional layer of encryption using RADIUS over Internet Protocol Security or RADIUS over Transport Layer Security.				Functional	subset of	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	10	
ISM-1457	N/A	Evaluated peripheral switches used for sharing peripherals between SECRET and TOP SECRET systems, or between SECRET or TOP SECRET systems belonging to different security domains, preferably complete a high assurance evaluation.				Functional	subset of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
ISM-1460	N/A	When using a software-based isolation mechanism to share a physical server's hardware, the isolation mechanism is from a vendor that has demonstrated a commitment to secure-by-design and secure-by-default principles, use of memory-safe programming languages where possible, secure programming practices, and maintaining the security of their products.				Functional	intersects with	Virtualization Techniques	SEA-13.1	Mechanisms exist to utilize virtualization techniques to support the employment of a diversity of operating systems and applications.	5	
ISM-1460	N/A	When using a software-based isolation mechanism to share a physical server's hardware, the isolation mechanism is from a vendor that has demonstrated a commitment to secure-by-design and secure-by-default principles, use of memory-safe programming languages where possible, secure programming practices, and maintaining the security of their products.				Functional	subset of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
ISM-1461	N/A	When using a software-based isolation mechanism to share a physical server's hardware for SECRET or TOP SECRET computing environments, the physical server and all computing environments are of the same classification and belong to the same security domain.				Functional	subset of	Virtualization Techniques	SEA-13.1	Mechanisms exist to utilize virtualization techniques to support the employment of a diversity of operating systems and applications.	10	
ISM-1467	N/A	The latest release of office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are used.				Functional	intersects with	Stable Versions	VPM-04.1	Mechanisms exist to install the latest stable version of any software and/or security-related updates on all applicable systems.	5	
ISM-1467	N/A	The latest release of office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are used.				Functional	intersects with	Automated Software & Firmware Updates	VPM-05.4	Automated mechanisms exist to install the latest stable versions of security-relevant software and firmware updates.	5	
ISM-1470	N/A	Unneeded components, services and functionality of office productivity suites, web browsers, email clients, PDF software and security products are disabled or removed.				Functional	subset of	Unsupported Internet Browsers & Email Clients	CFG-04.2	Mechanisms exist to allow only approved Internet browsers and email clients to run on systems.	10	
ISM-1471	N/A	When implementing application control using publisher certificate rules, publisher names and product names are used.				Functional	intersects with	Configuration Enforcement	CFG-06	Automated mechanisms exist to monitor, enforce and report on configurations for endpoint devices.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	Essential 8 ML1	Essential 8 ML1	Essential 8 ML1	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
ISM-1471	N/A	When implementing application control using publisher certificate rules, publisher names and product names are used.				Functional	intersects with	Integrity Assurance & Enforcement (IAE)	CFG-06.1	Automated mechanisms exist to identify unauthorized deviations from an approved baseline and implement automated resiliency actions to remediate the unauthorized change.	5	
ISM-1478	N/A	The CISO oversees their organisation's cyber security program and ensures their organisation's compliance with cyber security policy, standards, regulations and legislation.				Functional	subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	10	
ISM-1479	N/A	Servers minimise communications with other servers at the network and file system level.				Functional	subset of	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	10	
ISM-1480	N/A	Evaluated peripheral switches used for sharing peripherals between SECRET or TOP SECRET systems and any non-SECRET or TOP SECRET systems complete a high assurance evaluation.				Functional	subset of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
ISM-1482	N/A	Personnel accessing systems or data using an organisation-owned mobile device or desktop computer are either prohibited from using it for personal purposes or have enforced separation of work data from any personal data.				Functional	subset of	Personally-Owned Mobile Devices	MDM-06	Mechanisms exist to restrict the connection of personally-owned, mobile devices to organizational systems and networks.	10	
ISM-1483	N/A	The latest release of internet-facing server applications are used.				Functional	subset of	Stable Versions	VPM-04.1	Mechanisms exist to install the latest stable version of any software and/or security-related updates on all applicable systems.	10	
ISM-1485	N/A	Web browsers do not process web advertisements from the internet.	ML1	ML2	ML3	Functional	subset of	Unsupported Internet Browsers & Email Clients	CFG-04.2	Mechanisms exist to allow only approved Internet browsers and email clients to run on systems.	10	Essential Eight: ML1, ML2, ML3
ISM-1486	N/A	Web browsers do not process Java from the internet.	ML1	ML2	ML3	Functional	subset of	Unsupported Internet Browsers & Email Clients	CFG-04.2	Mechanisms exist to allow only approved Internet browsers and email clients to run on systems.	10	Essential Eight: ML1, ML2, ML3
ISM-1487	N/A	Only privileged users responsible for checking that Microsoft Office macros are free of malicious code can write to and modify content within Trusted Locations.			ML3	Functional	subset of	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	10	Essential Eight: ML3
ISM-1488	N/A	Microsoft Office macros in files originating from the internet are blocked.	ML1	ML2	ML3	Functional	subset of	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	10	Essential Eight: ML1, ML2, ML3
ISM-1489	N/A	Microsoft Office macro security settings cannot be changed by users.	ML1	ML2	ML3	Functional	subset of	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	10	Essential Eight: ML1, ML2, ML3
ISM-1490	N/A	Application control is implemented on internet-facing servers.		ML2	ML3	Functional	intersects with	Configuration Enforcement	CFG-06	Automated mechanisms exist to monitor, enforce and report on configurations for endpoint devices.	5	Essential Eight: ML2, ML3
ISM-1490	N/A	Application control is implemented on internet-facing servers.		ML2	ML3	Functional	intersects with	Integrity Assurance & Enforcement (IAE)	CFG-06.1	Automated mechanisms exist to identify unauthorized deviations from an approved baseline and implement automated resiliency actions to remediate the unauthorized change.	5	Essential Eight: ML2, ML3
ISM-1491	N/A	Unprivileged users are prevented from running script execution engines, including: - Windows Script Host (cscript.exe and wscript.exe) - PowerShell (powershell.exe, powershell_ise.exe and pwsh.exe) - Command Prompt (cmd.exe) - Windows Management Instrumentation (wmic.exe) - Microsoft Hypertext Markup Language (HTML) Application Host (mshta.exe).				Functional	subset of	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	10	
ISM-1492	N/A	Operating system exploit protection functionality is enabled.				Functional	subset of	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	10	
ISM-1493	N/A	Software registers for workstations, servers, network devices and other IT equipment are developed, implemented, maintained and verified on a regular basis.				Functional	intersects with	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to maintain a current list of approved technologies (hardware and software).	5	
ISM-1493	N/A	Software registers for workstations, servers, network devices and other IT equipment are developed, implemented, maintained and verified on a regular basis.				Functional	subset of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
ISM-1493	N/A	Software registers for workstations, servers, network devices and other IT equipment are developed, implemented, maintained and verified on a regular basis.				Functional	intersects with	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	5	
ISM-1501	N/A	Operating systems that are no longer supported by vendors are replaced.	ML1	ML2	ML3	Functional	equal	Unsupported Systems	TDA-17	Mechanisms exist to prevent unsupported systems by: (1) Replacing systems 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 system components required to satisfy mission/business needs.	10	Essential Eight: ML1, ML2, ML3
ISM-1502	N/A	Emails arriving via an external connection where the email source address uses an internal domain, or internal subdomain, are blocked at the email gateway.				Functional	subset of	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	10	
ISM-1504	N/A	Multi-factor authentication is used to authenticate users to their organisation's online services that process, store or communicate their organisation's sensitive data.	ML1	ML2	ML3	Functional	subset of	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	10	Essential Eight: ML1, ML2, ML3
ISM-1505	N/A	Multi-factor authentication is used to authenticate users of data repositories.			ML3	Functional	subset of	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	10	Essential Eight: ML3
ISM-1506	N/A	The use of SSH version 1 is disabled for SSH connections.				Functional	subset of	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	10	
ISM-1507	N/A	Requests for privileged access to systems, applications and data repositories are validated when first requested.	ML1	ML2	ML3	Functional	subset of	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.	10	Essential Eight: ML1, ML2, ML3
ISM-1508	N/A	Privileged access to systems, applications and data repositories is limited to only what is required for users and services to undertake their duties.			ML3	Functional	subset of	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.	10	Essential Eight: ML3
ISM-1509	N/A	Privileged access events are centrally logged.		ML2	ML3	Functional	subset of	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.	10	Essential Eight: ML2, ML3
ISM-1510	N/A	A digital preservation policy is developed, implemented and maintained.				Functional	intersects with	Retention Of Previous Configurations	CFG-02.3	Mechanisms exist to retain previous versions of baseline configuration to support roll back.	5	
ISM-1510	N/A	A digital preservation policy is developed, implemented and maintained.				Functional	intersects with	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	
ISM-1511	N/A	Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements.	ML1	ML2	ML3	Functional	equal	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 satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	10	Essential Eight: ML1, ML2, ML3
ISM-1515	N/A	Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises.	ML1	ML2	ML3	Functional	equal	Testing for Reliability & Integrity	BCD-11.1	Mechanisms exist to routinely test backups that verify the reliability of the backup process, as well as the integrity and availability of the data.	10	Essential Eight: ML1, ML2, ML3
ISM-1517	N/A	Equipment that is capable of reducing microform to a fine powder, with resultant particles not showing more than five consecutive characters per particle upon microscopic inspection, is used to destroy microfiche and microfilm.				Functional	subset of	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	10	
ISM-1520	N/A	System administrators for gateways undergo appropriate employment screening, and where necessary hold an appropriate security clearance, based on the sensitivity or classification of gateways.				Functional	subset of	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	10	
ISM-1521	N/A	CDSs implement protocol breaks at each network layer.				Functional	intersects with	Cross Domain Solution (CDS)	NET-02.3	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	5	
ISM-1521	N/A	CDSs implement protocol breaks at each network layer.				Functional	intersects with	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
ISM-1522	N/A	CDSs implement independent security-enforcing functions for upward and downward network paths.				Functional	intersects with	Cross Domain Solution (CDS)	NET-02.3	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	5	
ISM-1522	N/A	CDSs implement independent security-enforcing functions for upward and downward network paths.				Functional	intersects with	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
ISM-1523	N/A	A sample of security-relevant events relating to data transfer policies are taken at least every three months and assessed against security policies for CDSs to identify any operational failures.				Functional	subset of	Cross Domain Solution (CDS)	NET-02.3	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	10	
ISM-1524	N/A	Content filters used by CDSs undergo rigorous security testing to ensure they perform as expected and cannot be bypassed.				Functional	subset of	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	10	
ISM-1525	N/A	System owners register each system with its authorising officer.				Functional	subset of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy assessment and authorization controls.	10	
ISM-1525	N/A	System owners register each system with its authorising officer.				Functional	intersects with	Security Authorization	IAO-07	Mechanisms exist to ensure systems, projects and services are officially authorized prior to "go live" in a production environment.	5	
ISM-1526	N/A	System owners monitor each system, and associated cyber threats, security risks and controls, on an ongoing basis.				Functional	intersects with	Monitor Controls	GOV-15.5	Mechanisms exist to compel data and/or process owners to monitor systems, applications and/or services under their control on an ongoing basis for applicable threats and risks, as well as to ensure cybersecurity & data privacy controls are operating as intended.	5	
ISM-1526	N/A	System owners monitor each system, and associated cyber threats, security risks and controls, on an ongoing basis.				Functional	intersects with	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to systems within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
ISM-1526	N/A	System owners monitor each system, and associated cyber threats, security risks and controls, on an ongoing basis.				Functional	intersects with	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	Essential 8 ML1	Essential 8 ML1	Essential 8 ML1	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
ISM-1528	N/A	Evaluated firewalls are used between an organisation's networks and public network infrastructure.				Functional	subset of	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	10	
ISM-1529	N/A	Only community or private clouds are used for outsourced SECRET and TOP SECRET cloud services.				Functional	subset of	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	10	
ISM-1529	N/A	Only community or private clouds are used for outsourced SECRET and TOP SECRET cloud services.				Functional	intersects with	Multi-Tenant Environments	CLD-06	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	5	
ISM-1530	N/A	Servers, network devices and cryptographic equipment are secured in security containers or secure rooms suitable for their classification taking into account the combination of security zones they reside in.				Functional	subset of	Access To Information Systems	PES-03.4	Physical access control mechanisms exist to enforce physical access to critical information systems or sensitive/regulated data, in addition to the physical access controls for the facility.	10	
ISM-1532	N/A	VLANs are not used to separate network traffic between an organisation's networks and public network infrastructure.				Functional	subset of	Virtual Local Area Network (VLAN) Separation	NET-06.2	Mechanisms exist to enable Virtual Local Area Networks (VLANs) to limit the ability of devices on a network to directly communicate with other devices on the subnet and limit an attacker's ability to laterally move to compromise neighboring systems.	10	
ISM-1533	N/A	A mobile device management policy is developed, implemented and maintained.				Functional	subset of	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	10	
ISM-1534	N/A	Printer ribbons in printers and MFDs are removed and destroyed.				Functional	subset of	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	10	
ISM-1535	N/A	Processes, and supporting procedures, are developed, implemented and maintained to prevent AUSTEO, AGAO and REL data in textual and non-textual formats from being exported to unsuitable foreign systems.				Functional	subset of	Information Sharing	DCH-14	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	10	
ISM-1536	N/A	All queries to databases from web applications that are initiated by users, and any resulting crash or error messages, are centrally logged.				Functional	intersects with	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	
ISM-1536	N/A	All queries to databases from web applications that are initiated by users, and any resulting crash or error messages, are centrally logged.				Functional	intersects with	Content of Event Logs	MON-03	Mechanisms exist to configure systems to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5	
ISM-1537	N/A	The following events are centrally logged for databases: - Access or modification of particularly important content - Addition of new users, especially privileged users - Changes to user roles or privileges - Attempts to elevate user privileges - Queries containing comments - Queries containing multiple embedded queries - Database and query alerts or failures - Database structure changes - Database administrator actions - Use of executable commands - Database logons and logoffs.				Functional	intersects with	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	
ISM-1537	N/A	The following events are centrally logged for databases: - Access or modification of particularly important content - Addition of new users, especially privileged users - Changes to user roles or privileges - Attempts to elevate user privileges - Queries containing comments - Queries containing multiple embedded queries - Database and query alerts or failures - Database structure changes - Database administrator actions - Use of executable commands - Database logons and logoffs.				Functional	intersects with	Content of Event Logs	MON-03	Mechanisms exist to configure systems to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5	
ISM-1537	N/A	The following events are centrally logged for databases: - Access or modification of particularly important content - Addition of new users, especially privileged users - Changes to user roles or privileges - Attempts to elevate user privileges - Queries containing comments - Queries containing multiple embedded queries - Database and query alerts or failures - Database structure changes - Database administrator actions - Use of executable commands - Database logons and logoffs.				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-1537	N/A	The following events are centrally logged for databases: - Access or modification of particularly important content - Addition of new users, especially privileged users - Changes to user roles or privileges - Attempts to elevate user privileges - Queries containing comments - Queries containing multiple embedded queries - Database and query alerts or failures - Database structure changes - Database administrator actions - Use of executable commands - Database logons and logoffs.				Functional	intersects with	Database Logging	MON-03.7	Mechanisms exist to ensure databases produce audit records that contain sufficient information to monitor database activities.	5	
ISM-1540	N/A	DMARC records are configured for an organisation's domains (including subdomains) such that emails are rejected if they do not pass DMARC checks.				Functional	intersects with	Domain Name Service (DNS) Resolution	NET-10	Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.	5	
ISM-1540	N/A	DMARC records are configured for an organisation's domains (including subdomains) such that emails are rejected if they do not pass DMARC checks.				Functional	intersects with	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
ISM-1540	N/A	DMARC records are configured for an organisation's domains (including subdomains) such that emails are rejected if they do not pass DMARC checks.				Functional	intersects with	Domain-Based Message Authentication Reporting and Conformance (DMARC)	NET-20.4	Mechanisms exist to implement domain signature verification protections that authenticate incoming email according to the Domain-based Message Authentication Reporting and Conformance (DMARC).	5	
ISM-1542	N/A	Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.		ML2	ML3	Functional	subset of	Unsupported Internet Browsers & Email Clients	CFG-04.2	Mechanisms exist to allow only approved Internet browsers and email clients to run on systems.	10	Essential Eight: ML2, ML3
ISM-1543	N/A	An authorised RF and IR device register for SECRET and TOP SECRET areas is developed, implemented, maintained and verified on a regular basis.				Functional	subset of	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	10	
ISM-1544	N/A	Microsoft's recommended application blocklist is implemented.		ML2	ML3	Functional	intersects with	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5	Essential Eight: ML2, ML3
ISM-1544	N/A	Microsoft's recommended application blocklist is implemented.		ML2	ML3	Functional	intersects with	Configuration Enforcement	CFG-06	Automated mechanisms exist to monitor, enforce and report on configurations for endpoint devices.	5	Essential Eight: ML2, ML3
ISM-1544	N/A	Microsoft's recommended application blocklist is implemented.		ML2	ML3	Functional	intersects with	Integrity Assurance & Enforcement (IAE)	CFG-06.1	Automated mechanisms exist to identify unauthorized deviations from an approved baseline and implement automated resiliency actions to remediate the unauthorized change.	5	Essential Eight: ML2, ML3
ISM-1546	N/A	Users are authenticated before they are granted access to a system and its resources.				Functional	subset of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
ISM-1546	N/A	Users are authenticated before they are granted access to a system and its resources.				Functional	intersects with	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
ISM-1547	N/A	Data backup processes, and supporting data backup procedures, are developed, implemented and maintained.				Functional	subset of	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 satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	10	
ISM-1548	N/A	Data restoration processes, and supporting data restoration procedures, are developed, implemented and maintained.				Functional	subset of	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 satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	10	
ISM-1549	N/A	A media management policy is developed, implemented and maintained.				Functional	subset of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
ISM-1550	N/A	IT equipment disposal processes, and supporting IT equipment disposal procedures, are developed, implemented and maintained.				Functional	intersects with	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
ISM-1550	N/A	IT equipment disposal processes, and supporting IT equipment disposal procedures, are developed, implemented and maintained.				Functional	intersects with	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
ISM-1551	N/A	An IT equipment management policy is developed, implemented and maintained.				Functional	subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	10	
ISM-1552	N/A	All web application content is offered exclusively using HTTPS.				Functional	intersects with	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5	
ISM-1552	N/A	All web application content is offered exclusively using HTTPS.				Functional	intersects with	Secure Web Traffic	WEB-10	Mechanisms exist to ensure all web application content is delivered using cryptographic mechanisms (e.g., TLS).	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	Essential 8 ML1	Essential 8 ML1	Essential 8 ML1	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
ISM-1553	N/A	TLS compression is disabled for TLS connections.				Functional	subset of	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	10	
ISM-1554	N/A	If travelling overseas with mobile devices to high or extreme risk countries, personnel are: - issued with newly provisioned accounts, mobile devices and removable media from a pool of dedicated travel devices which are used solely for work-related activities - advised on how to apply and inspect tamper seals to key areas of mobile devices - advised to avoid taking any personal mobile devices, especially if rooted or jailbroken.				Functional	subset of	Travel-Only Devices	AST-24	Mechanisms exist to issue personnel travelling overseas with temporary, loaner or "travel-only" end user technology (e.g., laptops and mobile devices) when travelling to authoritarian countries with a higher-than average risk for Intellectual Property (IP) theft or espionage against individuals and private companies.	10	
ISM-1555	N/A	Before travelling overseas with mobile devices, personnel take the following actions: - record all details of the mobile devices being taken, such as product types, serial numbers and International Mobile Equipment Identity numbers - update all operating systems and applications - remove all non-essential data, applications and accounts - backup all remaining data, applications and settings.				Functional	subset of	Travel-Only Devices	AST-24	Mechanisms exist to issue personnel travelling overseas with temporary, loaner or "travel-only" end user technology (e.g., laptops and mobile devices) when travelling to authoritarian countries with a higher-than average risk for Intellectual Property (IP) theft or espionage against individuals and private companies.	10	
ISM-1556	N/A	If returning from travelling overseas with mobile devices to high or extreme risk countries, personnel take the following additional actions: - reset credentials used with mobile devices, including those used for remote access to their organisation's systems - monitor accounts for any indicators of compromise, such as failed logon attempts.				Functional	intersects with	Travel-Only Devices	AST-24	Mechanisms exist to issue personnel travelling overseas with temporary, loaner or "travel-only" end user technology (e.g., laptops and mobile devices) when travelling to authoritarian countries with a higher-than average risk for Intellectual Property (IP) theft or espionage against individuals and private companies.	5	
ISM-1556	N/A	If returning from travelling overseas with mobile devices to high or extreme risk countries, personnel take the following additional actions: - reset credentials used with mobile devices, including those used for remote access to their organisation's systems - monitor accounts for any indicators of compromise, such as failed logon attempts.				Functional	intersects with	Re-Imaging Devices After Travel	AST-25	Mechanisms exist to re-image end user technology (e.g., laptops and mobile devices) when returning from overseas travel to an authoritarian country with a higher-than average risk for Intellectual Property (IP) theft or espionage against individuals and private companies.	5	
ISM-1557	N/A	Passphrases used for single-factor authentication on SECRET systems are at least 5 random words with a total minimum length of 17 characters.				Functional	subset of	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	10	
ISM-1558	N/A	Passphrases used for single-factor authentication are not a list of categorised words; do not form a real sentence in a natural language; and are not constructed from song lyrics, movies, literature or any other publicly available material.				Functional	subset of	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	10	
ISM-1559	N/A	Memorised secrets used for multi-factor authentication are a minimum of 6 characters, unless more stringent requirements apply.				Functional	subset of	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	10	
ISM-1560	N/A	Memorised secrets used for multi-factor authentication on SECRET systems are a minimum of 8 characters.				Functional	subset of	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	10	
ISM-1561	N/A	Memorised secrets used for multi-factor authentication on TOP SECRET systems are a minimum of 10 characters.				Functional	subset of	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	10	
ISM-1562	N/A	Video conferencing and IP telephony infrastructure is hardened.				Functional	intersects with	Video Teleconference (VTC) Security	AST-20	Mechanisms exist to implement secure Video Teleconference (VTC) capabilities on endpoint devices and in designated conference rooms, to prevent potential eavesdropping.	5	
ISM-1562	N/A	Video conferencing and IP telephony infrastructure is hardened.				Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
ISM-1562	N/A	Video conferencing and IP telephony infrastructure is hardened.				Functional	intersects with	Use of Communications Technology	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously.	5	
ISM-1562	N/A	Video conferencing and IP telephony infrastructure is hardened.				Functional	intersects with	External Telecommunications Services	NET-03.2	Mechanisms exist to maintain a managed interface for each external telecommunication service that protects the confidentiality and integrity of the information being transmitted across each interface.	5	
ISM-1563	N/A	At the conclusion of a security assessment for a system, a security assessment report is produced by the assessor and covers: - the scope of the security assessment - the system's strengths and weaknesses - security risks associated with the operation of the system - the effectiveness of the implementation of controls - any recommended remediation actions.				Functional	subset of	Security Assessment Report (SAR)	IAO-02.4	Mechanisms exist to produce a Security Assessment Report (SAR) at the conclusion of a security assessment to certify the results of the assessment and assist with any remediation actions.	10	
ISM-1564	N/A	At the conclusion of a security assessment for a system, a plan of action and milestones is produced by the system owner.				Functional	intersects with	Plan of Action & Milestones (POA&M)	IAO-05	Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities.	5	
ISM-1565	N/A	Tailored privileged user training is undertaken annually by all privileged users.				Functional	intersects with	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
ISM-1565	N/A	Tailored privileged user training is undertaken annually by all privileged users.				Functional	intersects with	Privileged Users	SAT-03.5	Mechanisms exist to provide specific training for privileged users to ensure privileged users understand their unique roles and responsibilities	5	
ISM-1566	N/A	Use of unprivileged access is centrally logged.				Functional	subset of	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	10	
ISM-1567	N/A	Suppliers identified as high risk by a cyber supply chain risk assessment are not used.				Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
ISM-1567	N/A	Suppliers identified as high risk by a cyber supply chain risk assessment are not used.				Functional	intersects with	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with systems, system components and services.	5	
ISM-1567	N/A	Suppliers identified as high risk by a cyber supply chain risk assessment are not used.				Functional	intersects with	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique systems, system components or services.	5	
ISM-1567	N/A	Suppliers identified as high risk by a cyber supply chain risk assessment are not used.				Functional	intersects with	Limit Potential Harm	TPM-03.2	Mechanisms exist to utilize security safeguards to limit harm from potential adversaries who identify and target the organization's supply chain.	5	
ISM-1568	N/A	Applications, IT equipment, OT equipment and services are chosen from suppliers that have demonstrated a commitment to the security of their products and services.				Functional	intersects with	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique systems, system components or services.	5	
ISM-1568	N/A	Applications, IT equipment, OT equipment and services are chosen from suppliers that have demonstrated a commitment to the security of their products and services.				Functional	intersects with	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related services.	5	
ISM-1569	N/A	A shared responsibility model is created, documented and shared between suppliers and their customers in order to articulate the security responsibilities of each party.				Functional	intersects with	Supply Chain Coordination	IRO-10.4	Mechanisms exist to provide cybersecurity & data privacy incident information to the provider of the product or service and other organizations involved in the supply chain for systems or system components related to the incident.	5	
ISM-1569	N/A	A shared responsibility model is created, documented and shared between suppliers and their customers in order to articulate the security responsibilities of each party.				Functional	intersects with	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's systems and data.	5	
ISM-1569	N/A	A shared responsibility model is created, documented and shared between suppliers and their customers in order to articulate the security responsibilities of each party.				Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
ISM-1569	N/A	A shared responsibility model is created, documented and shared between suppliers and their customers in order to articulate the security responsibilities of each party.				Functional	intersects with	Third-Party Personnel Security	TPM-06	Mechanisms exist to control personnel security requirements including security roles and responsibilities for third-party providers.	5	
ISM-1570	N/A	Outsourced cloud service providers and their cloud services undergo a security assessment by an IRAP assessor at least every 24 months.				Functional	subset of	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; and/or (11) Artificial Intelligence and Autonomous Technologies (AAT).	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	Essential 8 ML1	Essential 8 ML1	Essential 8 ML1	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
ISM-1571	N/A	The right to verify compliance with security requirements is documented in contractual arrangements with service providers.				Functional	intersects with	Adequate Security for Sensitive / Regulated Data In Support of Contracts	IAO-03.2	Mechanisms exist to protect sensitive / regulated data that is collected, developed, received, transmitted, used or stored in support of the performance of a contract.	5	
ISM-1571	N/A	The right to verify compliance with security requirements is documented in contractual arrangements with service providers.				Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
ISM-1572	N/A	The regions or availability zones where data will be processed, stored and communicated, as well as a minimum notification period for any configuration changes, is documented in contractual arrangements with service providers.				Functional	intersects with	Geolocation Requirements for Processing, Storage and Service Locations	CLD-09	Mechanisms exist to control the location of cloud processing/storage based on business requirements that includes statutory, regulatory and contractual obligations.	5	
ISM-1572	N/A	The regions or availability zones where data will be processed, stored and communicated, as well as a minimum notification period for any configuration changes, is documented in contractual arrangements with service providers.				Functional	intersects with	Adequate Security for Sensitive / Regulated Data In Support of Contracts	IAO-03.2	Mechanisms exist to protect sensitive / regulated data that is collected, developed, received, transmitted, used or stored in support of the performance of a contract.	5	
ISM-1572	N/A	The regions or availability zones where data will be processed, stored and communicated, as well as a minimum notification period for any configuration changes, is documented in contractual arrangements with service providers.				Functional	intersects with	Third-Party Processing, Storage and Service Locations	TPM-04.4	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	5	
ISM-1572	N/A	The regions or availability zones where data will be processed, stored and communicated, as well as a minimum notification period for any configuration changes, is documented in contractual arrangements with service providers.				Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
ISM-1573	N/A	Access to all logs relating to an organisation's data and services is documented in contractual arrangements with service providers.				Functional	intersects with	Adequate Security for Sensitive / Regulated Data In Support of Contracts	IAO-03.2	Mechanisms exist to protect sensitive / regulated data that is collected, developed, received, transmitted, used or stored in support of the performance of a contract.	5	
ISM-1573	N/A	Access to all logs relating to an organisation's data and services is documented in contractual arrangements with service providers.				Functional	intersects with	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related services.	5	
ISM-1573	N/A	Access to all logs relating to an organisation's data and services is documented in contractual arrangements with service providers.				Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
ISM-1574	N/A	The storage of data in a portable manner that allows for backups, service migration and service decommissioning without any loss of data is documented in contractual arrangements with service providers.				Functional	intersects with	Adequate Security for Sensitive / Regulated Data In Support of Contracts	IAO-03.2	Mechanisms exist to protect sensitive / regulated data that is collected, developed, received, transmitted, used or stored in support of the performance of a contract.	5	
ISM-1574	N/A	The storage of data in a portable manner that allows for backups, service migration and service decommissioning without any loss of data is documented in contractual arrangements with service providers.				Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
ISM-1575	N/A	A minimum notification period of one month for the cessation of any services by a service provider is documented in contractual arrangements with service providers.				Functional	intersects with	Adequate Security for Sensitive / Regulated Data In Support of Contracts	IAO-03.2	Mechanisms exist to protect sensitive / regulated data that is collected, developed, received, transmitted, used or stored in support of the performance of a contract.	5	
ISM-1575	N/A	A minimum notification period of one month for the cessation of any services by a service provider is documented in contractual arrangements with service providers.				Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
ISM-1576	N/A	If an organisation's systems, applications or data are accessed or administered by a service provider in an unauthorised manner, the organisation is immediately notified.				Functional	subset of	Security Compromise Notification Agreements	TPM-05.1	Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely affected systems, applications and/or services that the organization utilizes.	10	
ISM-1577	N/A	An organisation's networks are segregated from their service providers' networks.				Functional	subset of	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	10	
ISM-1579	N/A	Cloud service providers' ability to dynamically scale resources in response to a genuine spike in demand is discussed and verified as part of capacity and availability planning for online services.				Functional	subset of	Capacity & Performance Management	CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	10	
ISM-1579	N/A	Cloud service providers' ability to dynamically scale resources in response to a genuine spike in demand is discussed and verified as part of capacity and availability planning for online services.				Functional	intersects with	Resource Priority	CAP-02	Mechanisms exist to control resource utilization of systems that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.	5	
ISM-1579	N/A	Cloud service providers' ability to dynamically scale resources in response to a genuine spike in demand is discussed and verified as part of capacity and availability planning for online services.				Functional	intersects with	Capacity Planning	CAP-03	Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.	5	
ISM-1579	N/A	Cloud service providers' ability to dynamically scale resources in response to a genuine spike in demand is discussed and verified as part of capacity and availability planning for online services.				Functional	intersects with	Elastic Expansion	CAP-05	Mechanisms exist to automatically scale the resources available for services, as demand conditions change.	5	
ISM-1579	N/A	Cloud service providers' ability to dynamically scale resources in response to a genuine spike in demand is discussed and verified as part of capacity and availability planning for online services.				Functional	subset of	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	10	
ISM-1580	N/A	Where a high availability requirement exists for online services, the services are architected to automatically transition between availability zones.				Functional	subset of	Capacity & Performance Management	CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	10	
ISM-1580	N/A	Where a high availability requirement exists for online services, the services are architected to automatically transition between availability zones.				Functional	intersects with	Resource Priority	CAP-02	Mechanisms exist to control resource utilization of systems that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.	5	
ISM-1580	N/A	Where a high availability requirement exists for online services, the services are architected to automatically transition between availability zones.				Functional	intersects with	Capacity Planning	CAP-03	Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.	5	
ISM-1580	N/A	Where a high availability requirement exists for online services, the services are architected to automatically transition between availability zones.				Functional	subset of	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	10	
ISM-1581	N/A	Continuous real-time monitoring of the capacity and availability of online services is performed.				Functional	subset of	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	10	
ISM-1581	N/A	Continuous real-time monitoring of the capacity and availability of online services is performed.				Functional	intersects with	Resource Priority	CAP-02	Mechanisms exist to control resource utilization of systems that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.	5	
ISM-1581	N/A	Continuous real-time monitoring of the capacity and availability of online services is performed.				Functional	subset of	Capacity & Performance Management	CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	10	
ISM-1581	N/A	Continuous real-time monitoring of the capacity and availability of online services is performed.				Functional	intersects with	Capacity Planning	CAP-03	Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.	5	
ISM-1582	N/A	Application control rulesets are validated on an annual or more frequent basis.		ML2	ML3	Functional	intersects with	Configuration Enforcement	CFG-06	Automated mechanisms exist to monitor, enforce and report on configurations for endpoint devices.	5	Essential Eight: ML2, ML3
ISM-1582	N/A	Application control rulesets are validated on an annual or more frequent basis.		ML2	ML3	Functional	intersects with	Integrity Assurance & Enforcement (IAE)	CFG-06.1	Automated mechanisms exist to identify unauthorized deviations from an approved baseline and implement automated resiliency actions to remediate the unauthorized change.	5	Essential Eight: ML2, ML3
ISM-1583	N/A	Personnel who are contractors are identified as such.				Functional	equal	Identification & Authentication for Non-Organizational Users	IAC-03	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization.	10	
ISM-1584	N/A	Unprivileged users are prevented from bypassing, disabling or modifying security functionality of operating systems.				Functional	subset of	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	10	
ISM-1585	N/A	Web browser security settings cannot be changed by users.	ML1	ML2	ML3	Functional	subset of	Unsupported Internet Browsers & Email Clients	CFG-04.2	Mechanisms exist to allow only approved Internet browsers and email clients to run on systems.	10	Essential Eight: ML1, ML2, ML3
ISM-1586	N/A	Data transfer logs are used to record all data imports and exports from systems.				Functional	subset of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
ISM-1587	N/A	System owners report the security status of each system to its authorising officer at least annually.				Functional	subset of	Cybersecurity & Data Privacy Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	10	
ISM-1588	N/A	SOEs are reviewed and updated at least annually.				Functional	subset of	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and upgrades.	10	
ISM-1589	N/A	MTA-STS is enabled to prevent the unencrypted transfer of emails between email servers.				Functional	intersects with	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
ISM-1589	N/A	MTA-STS is enabled to prevent the unencrypted transfer of emails between email servers.				Functional	intersects with	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
ISM-1590	N/A	Credentials are changed if: - they are compromised - they are suspected of being compromised - they are discovered stored on networks in the clear - they are discovered being transferred across networks in the clear - membership of a shared account changes - they have not been changed in the past 12 months.				Functional	subset of	Protection of Authenticators	IAC-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	10	
ISM-1591	N/A	Access to systems, applications and data repositories is removed or suspended as soon as practicable when personnel are detected undertaking malicious activities.				Functional	intersects with	Account Disabling for High Risk Individuals	IAC-15.6	Mechanisms exist to disable accounts immediately upon notification for users posing a significant risk to the organization.	5	
ISM-1591	N/A	Access to systems, applications and data repositories is removed or suspended as soon as practicable when personnel are detected undertaking malicious activities.				Functional	intersects with	Expeditious Disconnect / Disable Capability	NET-14.8	Mechanisms exist to provide the capability to expeditiously disconnect or disable a user's remote access session.	5	
ISM-1592	N/A	Unprivileged users do not have the ability to install unapproved software.				Functional	intersects with	User-Installed Software	CFG-05	Mechanisms exist to restrict the ability of non-privileged users to install unauthorized software.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	Essential 8 ML1	Essential 8 ML1	Essential 8 ML1	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
ISM-1592	N/A	Unprivileged users do not have the ability to install unapproved software.				Functional	intersects with	Restrict Roles Permitted To Install Software	CFG-05.2	Mechanisms exist to configure systems to prevent the installation of software, unless the action is performed by a privileged user or service.	5	
ISM-1592	N/A	Unprivileged users do not have the ability to install unapproved software.				Functional	intersects with	Prohibit Non-Privileged Users from Executing Privileged Functions	IAC-21.5	Mechanisms exist to prevent non-privileged users from executing privileged functions to include disabling, circumventing or altering implemented security safeguards / countermeasures.	5	
ISM-1593	N/A	Users provide sufficient evidence to verify their identity when requesting new credentials.				Functional	subset of	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	10	
ISM-1594	N/A	Credentials are provided to users via a secure communications channel or, if not possible, split into two parts with one part provided to users and the other part provided to supervisors.				Functional	subset of	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	10	
ISM-1595	N/A	Credentials provided to users are changed on first use.				Functional	subset of	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	10	
ISM-1596	N/A	Credentials, in the form of memorised secrets, are not reused by users across different systems.				Functional	subset of	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	10	
ISM-1597	N/A	Credentials are obscured as they are entered into systems.				Functional	subset of	Protection of Authenticators	IAC-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	10	
ISM-1598	N/A	Following maintenance or repair activities for IT equipment, the IT equipment is inspected to confirm it retains its approved software configuration and that no unauthorised modifications have taken place.				Functional	equal	Maintenance Validation	MNT-10	Mechanisms exist to validate maintenance activities were appropriately performed according to the work order and that security controls are operational.	10	
ISM-1599	N/A	IT equipment is handled in a manner suitable for its sensitivity or classification.				Functional	subset of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
ISM-1599	N/A	IT equipment is handled in a manner suitable for its sensitivity or classification.				Functional	intersects with	Component Marking	PES-16	Physical security mechanisms exist to mark system hardware components indicating the impact or classification level of the information permitted to be processed, stored or transmitted by the hardware component.	5	
ISM-1600	N/A	Media is sanitised before it is used for the first time.				Functional	intersects with	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
ISM-1600	N/A	Media is sanitised before it is used for the first time.				Functional	intersects with	First Time Use Sanitization	DCH-09.4	Mechanisms exist to apply nondestructive sanitization techniques to portable storage devices prior to first use.	5	
ISM-1601	N/A	Microsoft's attack surface reduction rules are implemented.				Functional	subset of	Unsupported Internet Browsers & Email Clients	CFG-04.2	Mechanisms exist to allow only approved Internet browsers and email clients to run on systems.	10	
ISM-1602	N/A	Security documentation, including notification of subsequent changes, is communicated to all stakeholders.				Functional	subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	10	
ISM-1603	N/A	Authentication methods susceptible to replay attacks are disabled.				Functional	intersects with	Replay-Resistant Authentication	IAC-02.2	Automated mechanisms exist to employ replay-resistant authentication.	5	
ISM-1603	N/A	Authentication methods susceptible to replay attacks are disabled.				Functional	intersects with	Identification & Authentication for Devices	IAC-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically- based and replay resistant.	5	
ISM-1604	N/A	When using a software-based isolation mechanism to share a physical server's hardware, the configuration of the isolation mechanism is hardened by removing unneeded functionality and restricting access to the administrative interface used to manage the isolation mechanism.				Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
ISM-1604	N/A	When using a software-based isolation mechanism to share a physical server's hardware, the configuration of the isolation mechanism is hardened by removing unneeded functionality and restricting access to the administrative interface used to manage the isolation mechanism.				Functional	intersects with	Virtualization Techniques	SEA-13.1	Mechanisms exist to utilize virtualization techniques to support the employment of a diversity of operating systems and applications.	5	
ISM-1605	N/A	When using a software-based isolation mechanism to share a physical server's hardware, the underlying operating system is hardened.				Functional	subset of	Virtualization Techniques	SEA-13.1	Mechanisms exist to utilize virtualization techniques to support the employment of a diversity of operating systems and applications.	10	
ISM-1606	N/A	When using a software-based isolation mechanism to share a physical server's hardware, patches, updates or vendor mitigations for vulnerabilities are applied to the isolation mechanism and underlying operating system in a timely manner.				Functional	subset of	Virtualization Techniques	SEA-13.1	Mechanisms exist to utilize virtualization techniques to support the employment of a diversity of operating systems and applications.	10	
ISM-1607	N/A	When using a software-based isolation mechanism to share a physical server's hardware, integrity and log monitoring are performed for the isolation mechanism and underlying operating system in a timely manner.				Functional	subset of	Virtualization Techniques	SEA-13.1	Mechanisms exist to utilize virtualization techniques to support the employment of a diversity of operating systems and applications.	10	
ISM-1608	N/A	SOEs provided by third parties are scanned for malicious code and configurations.				Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
ISM-1608	N/A	SOEs provided by third parties are scanned for malicious code and configurations.				Functional	intersects with	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
ISM-1608	N/A	SOEs provided by third parties are scanned for malicious code and configurations.				Functional	intersects with	Heuristic / Nonsignature-Based Detection	END-04.4	Mechanisms exist to utilize heuristic / nonsignature-based antimalware detection capabilities.	5	
ISM-1609	N/A	System owners are consulted before allowing intrusion activity to continue on a system for the purpose of collecting further data or evidence.				Functional	subset of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	10	
ISM-1609	N/A	System owners are consulted before allowing intrusion activity to continue on a system for the purpose of collecting further data or evidence.				Functional	intersects with	Chain of Custody & Forensics	IRO-08	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	5	
ISM-1609	N/A	System owners are consulted before allowing intrusion activity to continue on a system for the purpose of collecting further data or evidence.				Functional	intersects with	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity & data privacy incidents to internal stakeholders all the way through the resolution of the incident.	5	
ISM-1609	N/A	System owners are consulted before allowing intrusion activity to continue on a system for the purpose of collecting further data or evidence.				Functional	intersects with	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.	5	
ISM-1610	N/A	A method of emergency access to systems is documented and tested at least once when initially implemented and each time fundamental information technology infrastructure changes occur.				Functional	subset of	Emergency Accounts	IAC-15.9	Mechanisms exist to establish and control "emergency access only" accounts.	10	
ISM-1611	N/A	Break glass accounts are only used when normal authentication processes cannot be used.				Functional	subset of	Emergency Accounts	IAC-15.9	Mechanisms exist to establish and control "emergency access only" accounts.	10	
ISM-1612	N/A	Break glass accounts are only used for specific authorised activities.				Functional	subset of	Emergency Accounts	IAC-15.9	Mechanisms exist to establish and control "emergency access only" accounts.	10	
ISM-1613	N/A	Use of break glass accounts is centrally logged.				Functional	subset of	Emergency Accounts	IAC-15.9	Mechanisms exist to establish and control "emergency access only" accounts.	10	
ISM-1614	N/A	Break glass account credentials are changed by the account custodian after they are accessed by any other party.				Functional	subset of	Emergency Accounts	IAC-15.9	Mechanisms exist to establish and control "emergency access only" accounts.	10	
ISM-1615	N/A	Break glass accounts are tested after credentials are changed.				Functional	subset of	Emergency Accounts	IAC-15.9	Mechanisms exist to establish and control "emergency access only" accounts.	10	
ISM-1616	N/A	A vulnerability disclosure program is implemented to assist with the secure development and maintenance of products and services.				Functional	equal	Vulnerability Disclosure Program (VDP)	THR-06	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of products and services that receives unsolicited input from the public about vulnerabilities in organizational systems, services and processes.	10	
ISM-1617	N/A	The CISO regularly reviews and updates their organisation's cyber security program to ensure its relevance in addressing cyber threats and harnessing business and cyber security opportunities.				Functional	equal	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	10	
ISM-1618	N/A	The CISO oversees their organisation's response to cyber security incidents.				Functional	subset of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	10	
ISM-1618	N/A	The CISO oversees their organisation's response to cyber security incidents.				Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
ISM-1618	N/A	The CISO oversees their organisation's response to cyber security incidents.				Functional	intersects with	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity & data privacy incident response operations.	5	
ISM-1619	N/A	Service accounts are created as group Managed Service Accounts.				Functional	subset of	Group Authentication	IAC-02.1	Mechanisms exist to require individuals to be authenticated with an individual authenticator when a group authenticator is utilized.	10	
ISM-1620	N/A	Privileged user accounts are members of the Protected Users security group.				Functional	subset of	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.	10	
ISM-1621	N/A	Windows PowerShell 2.0 is disabled or removed.			ML3	Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	Essential Eight: ML3
ISM-1621	N/A	Windows PowerShell 2.0 is disabled or removed.			ML3	Functional	intersects with	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5	Essential Eight: ML3
ISM-1622	N/A	PowerShell is configured to use Constrained Language Mode.			ML3	Functional	subset of	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	10	Essential Eight: ML3

FDE #	FDE Name	Focal Document Element (FDE) Description	Essential 8 ML1	Essential 8 ML1	Essential 8 ML1	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
ISM-1623	N/A	PowerShell module logging, script block logging and transcription events are centrally logged.		ML2	ML3	Functional	subset of	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	10	Essential Eight: ML2, ML3
ISM-1624	N/A	PowerShell script block logs are protected by Protected Event Logging functionality.				Functional	subset of	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	10	
ISM-1625	N/A	An insider threat mitigation program is developed, implemented and maintained.				Functional	intersects with	Insider Threat Response Capability	IRO-02.2	Mechanisms exist to implement and govern an insider threat program.	5	
ISM-1625	N/A	An insider threat mitigation program is developed, implemented and maintained.				Functional	intersects with	Insider Threats	MON-16.1	Mechanisms exist to monitor internal personnel activity for potential security incidents.	5	
ISM-1625	N/A	An insider threat mitigation program is developed, implemented and maintained.				Functional	intersects with	Insider Threat Program	THR-04	Mechanisms exist to implement an insider threat program that includes a cross-discipline insider threat incident handling team.	5	
ISM-1625	N/A	An insider threat mitigation program is developed, implemented and maintained.				Functional	intersects with	Insider Threat Awareness	THR-05	Mechanisms exist to utilize security awareness training on recognizing and reporting potential indicators of insider threat.	5	
ISM-1626	N/A	Legal advice is sought regarding the development and implementation of an insider threat mitigation program.				Functional	intersects with	Insider Threat Response Capability	IRO-02.2	Mechanisms exist to implement and govern an insider threat program.	5	
ISM-1626	N/A	Legal advice is sought regarding the development and implementation of an insider threat mitigation program.				Functional	intersects with	Insider Threat Program	THR-04	Mechanisms exist to implement an insider threat program that includes a cross-discipline insider threat incident handling team.	5	
ISM-1626	N/A	Legal advice is sought regarding the development and implementation of an insider threat mitigation program.				Functional	intersects with	Insider Threat Awareness	THR-05	Mechanisms exist to utilize security awareness training on recognizing and reporting potential indicators of insider threat.	5	
ISM-1627	N/A	Inbound network connections from anonymity networks are blocked.				Functional	subset of	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-08	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	10	
ISM-1628	N/A	Outbound network connections to anonymity networks are blocked.				Functional	subset of	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-08	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	10	
ISM-1629	N/A	When using DH for agreeing on encryption session keys, a modulus and associated parameters are selected according to NIST SP 800-56A Rev. 3.				Functional	subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
ISM-1631	N/A	Suppliers of applications, IT equipment, OT equipment and services associated with systems are identified.				Functional	subset of	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's systems, applications, services and data.	10	
ISM-1632	N/A	Applications, IT equipment, OT equipment and services are chosen from suppliers that have a strong track record of maintaining the security of their own systems and cyber supply chains.				Functional	intersects with	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with the services and product supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5	
ISM-1632	N/A	Applications, IT equipment, OT equipment and services are chosen from suppliers that have a strong track record of maintaining the security of their own systems and cyber supply chains.				Functional	intersects with	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique systems, system components or services.	5	
ISM-1633	N/A	System owners determine the type, value and security objectives for each system based on an assessment of the impact if it were to be compromised.				Functional	subset of	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	10	
ISM-1634	N/A	System owners select controls for each system and tailor them to achieve desired security objectives.				Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
ISM-1634	N/A	System owners select controls for each system and tailor them to achieve desired security objectives.				Functional	intersects with	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required cybersecurity & data privacy controls for each system, application and/or service under their control.	5	
ISM-1635	N/A	System owners implement controls for each system and its operating environment.				Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
ISM-1635	N/A	System owners implement controls for each system and its operating environment.				Functional	intersects with	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required cybersecurity & data privacy controls for each system, application and/or service under their control.	5	
ISM-1636	N/A	System owners ensure controls for each system and its operating environment are assessed to determine if they have been implemented correctly and are operating as intended.				Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
ISM-1636	N/A	System owners ensure controls for each system and its operating environment are assessed to determine if they have been implemented correctly and are operating as intended.				Functional	intersects with	Assess Controls	GOV-15.3	Mechanisms exist to compel data and/or process owners to assess if required cybersecurity & data privacy controls for each system, application and/or service under their control are implemented correctly and are operating as intended.	5	
ISM-1637	N/A	An outsourced cloud service register is developed, implemented, maintained and verified on a regular basis.				Functional	subset of	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's systems, applications, services and data.	10	
ISM-1638	N/A	An outsourced cloud service register contains the following for each outsourced cloud service: - Cloud service provider's name - Cloud service's name - Purpose for using the cloud service - Sensitivity or classification of data involved - Due date for the next security assessment of the cloud service - Contractual arrangements for the cloud service - Point of contact for users of the cloud service - 24/7 contact details for the cloud service provider.				Functional	subset of	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's systems, applications, services and data.	10	
ISM-1639	N/A	Building management cables are labelled with their purpose in black writing on a yellow background, with a minimum size of 2.5 cm x 1 cm, and attached at five-metre intervals.				Functional	subset of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
ISM-1640	N/A	Cables for foreign systems installed in Australian facilities are labelled at inspection points.				Functional	subset of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
ISM-1641	N/A	Following the use of a degausser, magnetic media is physically damaged by deforming any internal platters.				Functional	subset of	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	10	
ISM-1642	N/A	Media is sanitised before it is reused in a different security domain.				Functional	subset of	First Time Use Sanitization	DCH-09.4	Mechanisms exist to apply nondestructive sanitization techniques to portable storage devices prior to first use.	10	
ISM-1643	N/A	Software registers contain versions and patch histories of applications, drivers, operating systems and firmware.				Functional	subset of	Asset Inventories	AST-02	Mechanisms exist to maintain a current list of approved technologies (hardware and software).	10	
ISM-1644	N/A	Sensitive or classified phone calls are not conducted in public locations unless care is taken to reduce the chance of conversations being overheard.				Functional	intersects with	Use of Communications Technology	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously.	5	
ISM-1644	N/A	Sensitive or classified phone calls are not conducted in public locations unless care is taken to reduce the chance of conversations being overheard.				Functional	intersects with	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	5	
ISM-1645	N/A	Floor plan diagrams are developed, implemented, maintained and verified on a regular basis.				Functional	subset of	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive/regulated data flows.	10	
ISM-1646	N/A	Floor plan diagrams contain the following: - cable paths (including ingress and egress points between floors) - cable reticulation system and conduit paths - floor concentration boxes - wall outlet boxes - network cabinets.				Functional	subset of	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive/regulated data flows.	10	
ISM-1647	N/A	Privileged access to systems, applications and data repositories is disabled after 12 months unless revalidated.		ML2	ML3	Functional	subset of	Periodic Review of Account Privileges	IAC-17	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	10	Essential Eight: ML2, ML3
ISM-1648	N/A	Privileged access to systems and applications is disabled after 45 days of inactivity.		ML2	ML3	Functional	intersects with	Disable Inactive Accounts	IAC-15.3	Automated mechanisms exist to disable inactive accounts after an organization-defined time period.	5	Essential Eight: ML2, ML3
ISM-1648	N/A	Privileged access to systems and applications is disabled after 45 days of inactivity.		ML2	ML3	Functional	intersects with	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.	5	Essential Eight: ML2, ML3
ISM-1648	N/A	Privileged access to systems and applications is disabled after 45 days of inactivity.		ML2	ML3	Functional	intersects with	Periodic Review of Account Privileges	IAC-17	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	5	Essential Eight: ML2, ML3
ISM-1649	N/A	Just-in-time administration is used for administering systems and applications.			ML3	Functional	intersects with	Automated System Account Management (Directory Services)	IAC-15.1	Automated mechanisms exist to support the management of system accounts (e.g., directory services).	5	Essential Eight: ML3
ISM-1649	N/A	Just-in-time administration is used for administering systems and applications.			ML3	Functional	intersects with	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.	5	Essential Eight: ML3
ISM-1650	N/A	Privileged account and group management events are centrally logged.		ML2	ML3	Functional	intersects with	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.	5	Essential Eight: ML2, ML3
ISM-1650	N/A	Privileged account and group management events are centrally logged.		ML2	ML3	Functional	intersects with	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	Essential Eight: ML2, ML3
ISM-1650	N/A	Privileged account and group management events are centrally logged.		ML2	ML3	Functional	intersects with	Account Creation and Modification Logging	MON-16.4	Automated mechanisms exist to generate event logs for permissions changes to privileged accounts and/or groups.	5	Essential Eight: ML2, ML3
ISM-1654	N/A	Internet Explorer 11 is disabled or removed.	ML1	ML2	ML3	Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	Essential Eight: ML1, ML2, ML3
ISM-1654	N/A	Internet Explorer 11 is disabled or removed.	ML1	ML2	ML3	Functional	intersects with	Unsupported Internet Browsers & Email Clients	CFG-04.2	Mechanisms exist to allow only approved Internet browsers and email clients to run on systems.	5	Essential Eight: ML1, ML2, ML3

FDE #	FDE Name	Focal Document Element (FDE) Description	Essential 8 ML1	Essential 8 ML1	Essential 8 ML1	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
ISM-1655	N/A	.NET Framework 3.5 (includes .NET 2.0 and 3.0) is disabled or removed.			ML3	Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	Essential Eight: ML3
ISM-1655	N/A	.NET Framework 3.5 (includes .NET 2.0 and 3.0) is disabled or removed.			ML3	Functional	intersects with	Unsupported Internet Browsers & Email Clients	CFG-04.2	Mechanisms exist to allow only approved Internet browsers and email clients to run on systems.	5	Essential Eight: ML3
ISM-1655	N/A	.NET Framework 3.5 (includes .NET 2.0 and 3.0) is disabled or removed.			ML3	Functional	intersects with	User-Installed Software	CFG-05	Mechanisms exist to restrict the ability of non-privileged users to install unauthorized software.	5	Essential Eight: ML3
ISM-1656	N/A	Application control is implemented on non-internet-facing servers.			ML3	Functional	subset of	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	10	Essential Eight: ML3
ISM-1657	N/A	Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.	ML1	ML2	ML3	Functional	subset of	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	10	Essential Eight: ML1, ML2, ML3
ISM-1658	N/A	Application control restricts the execution of drivers to an organisation-approved set.			ML3	Functional	subset of	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	10	Essential Eight: ML3
ISM-1659	N/A	Microsoft's vulnerable driver blocklist is implemented.			ML3	Functional	subset of	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	10	Essential Eight: ML3
ISM-1660	N/A	Allowed and blocked application control events are centrally logged.		ML2	ML3	Functional	intersects with	Monitoring Reporting	MON-06	Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.	5	Essential Eight: ML2, ML3
ISM-1660	N/A	Allowed and blocked application control events are centrally logged.		ML2	ML3	Functional	intersects with	Anomalous Behavior	MON-16	Mechanisms exist to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5	Essential Eight: ML2, ML3
ISM-1667	N/A	Microsoft Office is blocked from creating child processes.		ML2	ML3	Functional	subset of	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	10	Essential Eight: ML2, ML3
ISM-1668	N/A	Microsoft Office is blocked from creating executable content.		ML2	ML3	Functional	subset of	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	10	Essential Eight: ML2, ML3
ISM-1669	N/A	Microsoft Office is blocked from injecting code into other processes.		ML2	ML3	Functional	subset of	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	10	Essential Eight: ML2, ML3
ISM-1670	N/A	PDF software is blocked from creating child processes.		ML2	ML3	Functional	subset of	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	10	Essential Eight: ML2, ML3
ISM-1671	N/A	Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.	ML1	ML2	ML3	Functional	subset of	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	10	Essential Eight: ML1, ML2, ML3
ISM-1672	N/A	Microsoft Office macro antivirus scanning is enabled.	ML1	ML2	ML3	Functional	subset of	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	10	Essential Eight: ML1, ML2, ML3
ISM-1673	N/A	Microsoft Office macros are blocked from making Win32 API calls.		ML2	ML3	Functional	subset of	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	10	Essential Eight: ML2, ML3
ISM-1674	N/A	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.			ML3	Functional	subset of	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	10	Essential Eight: ML3
ISM-1675	N/A	Microsoft Office macros digitally signed by an untrusted publisher cannot be enabled via the Message Bar or Backstage View.			ML3	Functional	subset of	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	10	Essential Eight: ML3
ISM-1676	N/A	Microsoft Office's list of trusted publishers is validated on an annual or more frequent basis.			ML3	Functional	subset of	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	10	Essential Eight: ML3
ISM-1677	N/A	Allowed and blocked Microsoft Office macro execution events are centrally logged.				Functional	subset of	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	10	
ISM-1679	N/A	Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation's sensitive data.	ML1	ML2	ML3	Functional	subset of	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	10	Essential Eight: ML1, ML2, ML3
ISM-1680	N/A	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.	ML1	ML2	ML3	Functional	subset of	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	10	Essential Eight: ML1, ML2, ML3
ISM-1681	N/A	Multi-factor authentication is used to authenticate customers to online customer services that process, store or communicate sensitive customer data.	ML1	ML2	ML3	Functional	subset of	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	10	Essential Eight: ML1, ML2, ML3
ISM-1682	N/A	Multi-factor authentication used for authenticating users of systems is phishing-resistant.		ML2	ML3	Functional	subset of	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	10	Essential Eight: ML2, ML3
ISM-1683	N/A	Successful and unsuccessful multi-factor authentication events are centrally logged.		ML2	ML3	Functional	subset of	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	10	Essential Eight: ML2, ML3
ISM-1685	N/A	Credentials for break glass accounts, local administrator accounts and service accounts are long, unique, unpredictable and managed.		ML2	ML3	Functional	subset of	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	10	Essential Eight: ML2, ML3
ISM-1686	N/A	Credential Guard functionality is enabled.			ML3	Functional	subset of	Protection of Authenticators	IAC-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	10	Essential Eight: ML3
ISM-1687	N/A	Privileged operating environments are not virtualised within unprivileged operating environments.		ML2	ML3	Functional	subset of	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.	10	Essential Eight: ML2, ML3
ISM-1688	N/A	Unprivileged accounts cannot logon to privileged operating environments.	ML1	ML2	ML3	Functional	subset of	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.	10	Essential Eight: ML1, ML2, ML3
ISM-1689	N/A	Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.	ML1	ML2	ML3	Functional	subset of	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.	10	Essential Eight: ML1, ML2, ML3
ISM-1690	N/A	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.	ML1	ML2	ML3	Functional	subset of	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	10	Essential Eight: ML1, ML2, ML3
ISM-1691	N/A	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.	ML1	ML2		Functional	subset of	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	10	Essential Eight: ML1, ML2
ISM-1692	N/A	Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.			ML3	Functional	subset of	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	10	Essential Eight: ML3
ISM-1693	N/A	Patches, updates or other vendor mitigations for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release.		ML2	ML3	Functional	subset of	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	10	Essential Eight: ML2, ML3
ISM-1694	N/A	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.	ML1	ML2	ML3	Functional	subset of	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	10	Essential Eight: ML1, ML2, ML3
ISM-1695	N/A	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.	ML1	ML2		Functional	subset of	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	10	Essential Eight: ML1, ML2
ISM-1696	N/A	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.			ML3	Functional	subset of	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	10	Essential Eight: ML3
ISM-1697	N/A	Patches, updates or other vendor mitigations for vulnerabilities in drivers are applied within one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.			ML3	Functional	subset of	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	10	Essential Eight: ML3
ISM-1698	N/A	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services.	ML1	ML2	ML3	Functional	subset of	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	10	Essential Eight: ML1, ML2, ML3
ISM-1699	N/A	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.	ML1	ML2	ML3	Functional	subset of	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	10	Essential Eight: ML1, ML2, ML3

FDE #	FDE Name	Focal Document Element (FDE) Description	Essential 8 ML1	Essential 8 ML1	Essential 8 ML1	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
ISM-1700	N/A	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.		ML2	ML3	Functional	subset of	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	10	Essential Eight: ML2, ML3
ISM-1701	N/A	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices.	ML1	ML2	ML3	Functional	subset of	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	10	Essential Eight: ML1, ML2, ML3
ISM-1702	N/A	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices.	ML1	ML2	ML3	Functional	subset of	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	10	Essential Eight: ML1, ML2, ML3
ISM-1703	N/A	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in drivers.			ML3	Functional	subset of	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	10	Essential Eight: ML3
ISM-1704	N/A	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.	ML1	ML2	ML3	Functional	subset of	Unsupported Systems	TDA-17	Mechanisms exist to prevent unsupported systems by: (1) Replacing systems 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 system components required to satisfy mission/business needs.	10	Essential Eight: ML1, ML2, ML3
ISM-1705	N/A	Privileged accounts (excluding backup administrator accounts) cannot access backups belonging to other accounts.		ML2	ML3	Functional	subset of	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	10	Essential Eight: ML2, ML3
ISM-1706	N/A	Privileged accounts (excluding backup administrator accounts) cannot access their own backups.			ML3	Functional	subset of	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	10	Essential Eight: ML3
ISM-1707	N/A	Privileged accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups.		ML2	ML3	Functional	subset of	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	10	Essential Eight: ML2, ML3
ISM-1708	N/A	Backup administrator accounts are prevented from modifying and deleting backups during their retention period.			ML3	Functional	subset of	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	10	Essential Eight: ML3
ISM-1710	N/A	Settings for wireless access points are hardened.				Functional	subset of	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	10	
ISM-1711	N/A	User identity confidentiality is used if available with EAP-TLS implementations.				Functional	subset of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
ISM-1712	N/A	The use of FT (802.11r) is disabled unless authenticator-to-authenticator communications are secured by an ASD- Approved Cryptographic Protocol.				Functional	subset of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	Fast Basic Service Set Transition (FT) (802.11r)
ISM-1713	N/A	A removable media register is developed, implemented, maintained and verified on a regular basis.				Functional	subset of	Removable Media Security	DCH-12	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	10	
ISM-1716	N/A	Access to data repositories is disabled after 45 days of inactivity.				Functional	subset of	Periodic Review of Account Privileges	IAC-17	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	10	
ISM-1717	N/A	A 'security.txt' file is hosted for all internet-facing organisational domains to assist in the responsible disclosure of vulnerabilities in an organisation's products and services.				Functional	subset of	Vulnerability Disclosure Program (VDP)	THR-06	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of products and services that receives unsolicited input from the public about vulnerabilities in organizational systems, services and processes.	10	
ISM-1718	N/A	SECRET cables are coloured salmon pink.				Functional	intersects with	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
ISM-1718	N/A	SECRET cables are coloured salmon pink.				Functional	intersects with	Component Marking	PES-16	Physical security mechanisms exist to mark system hardware components indicating the impact or classification level of the information permitted to be processed, stored or transmitted by the hardware component.	5	
ISM-1719	N/A	TOP SECRET cables are coloured red.				Functional	intersects with	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
ISM-1719	N/A	TOP SECRET cables are coloured red.				Functional	intersects with	Component Marking	PES-16	Physical security mechanisms exist to mark system hardware components indicating the impact or classification level of the information permitted to be processed, stored or transmitted by the hardware component.	5	
ISM-1720	N/A	SECRET wall outlet boxes are coloured salmon pink.				Functional	intersects with	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
ISM-1720	N/A	SECRET wall outlet boxes are coloured salmon pink.				Functional	intersects with	Component Marking	PES-16	Physical security mechanisms exist to mark system hardware components indicating the impact or classification level of the information permitted to be processed, stored or transmitted by the hardware component.	5	
ISM-1721	N/A	TOP SECRET wall outlet boxes are coloured red.				Functional	intersects with	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
ISM-1721	N/A	TOP SECRET wall outlet boxes are coloured red.				Functional	intersects with	Component Marking	PES-16	Physical security mechanisms exist to mark system hardware components indicating the impact or classification level of the information permitted to be processed, stored or transmitted by the hardware component.	5	
ISM-1722	N/A	Electrostatic memory devices are destroyed using a furnace/incinerator, hammer mill, disintegrator or grinder/sander.				Functional	intersects with	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
ISM-1722	N/A	Electrostatic memory devices are destroyed using a furnace/incinerator, hammer mill, disintegrator or grinder/sander.				Functional	intersects with	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
ISM-1723	N/A	Magnetic floppy disks are destroyed using a furnace/incinerator, hammer mill, disintegrator, degausser or by cutting.				Functional	intersects with	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
ISM-1723	N/A	Magnetic floppy disks are destroyed using a furnace/incinerator, hammer mill, disintegrator, degausser or by cutting.				Functional	intersects with	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
ISM-1724	N/A	Magnetic hard disks are destroyed using a furnace/incinerator, hammer mill, disintegrator, grinder/sander or degausser.				Functional	intersects with	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
ISM-1724	N/A	Magnetic hard disks are destroyed using a furnace/incinerator, hammer mill, disintegrator, grinder/sander or degausser.				Functional	intersects with	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
ISM-1725	N/A	Magnetic tapes are destroyed using a furnace/incinerator, hammer mill, disintegrator, degausser or by cutting.				Functional	intersects with	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
ISM-1725	N/A	Magnetic tapes are destroyed using a furnace/incinerator, hammer mill, disintegrator, degausser or by cutting.				Functional	intersects with	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
ISM-1726	N/A	Optical disks are destroyed using a furnace/incinerator, hammer mill, disintegrator, grinder/sander or by cutting.				Functional	intersects with	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
ISM-1726	N/A	Optical disks are destroyed using a furnace/incinerator, hammer mill, disintegrator, grinder/sander or by cutting.				Functional	intersects with	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
ISM-1727	N/A	Semiconductor memory is destroyed using a furnace/incinerator, hammer mill or disintegrator.				Functional	intersects with	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
ISM-1727	N/A	Semiconductor memory is destroyed using a furnace/incinerator, hammer mill or disintegrator.				Functional	intersects with	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
ISM-1728	N/A	The resulting media waste particles from the destruction of SECRET media is stored and handled as OFFICIAL if less than or equal to 3 mm, PROTECTED if greater than 3 mm and less than or equal to 6 mm, or SECRET if greater than 6 mm and less than or equal to 9 mm.				Functional	intersects with	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
ISM-1728	N/A	The resulting media waste particles from the destruction of SECRET media is stored and handled as OFFICIAL if less than or equal to 3 mm, PROTECTED if greater than 3 mm and less than or equal to 6 mm, or SECRET if greater than 6 mm and less than or equal to 9 mm.				Functional	intersects with	Component Marking	PES-16	Physical security mechanisms exist to mark system hardware components indicating the impact or classification level of the information permitted to be processed, stored or transmitted by the hardware component.	5	
ISM-1729	N/A	The resulting media waste particles from the destruction of TOP SECRET media is stored and handled as OFFICIAL if less than or equal to 3 mm, or SECRET if greater than 3 mm and less than or equal to 9 mm.				Functional	intersects with	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
ISM-1729	N/A	The resulting media waste particles from the destruction of TOP SECRET media is stored and handled as OFFICIAL if less than or equal to 3 mm, or SECRET if greater than 3 mm and less than or equal to 9 mm.				Functional	intersects with	Component Marking	PES-16	Physical security mechanisms exist to mark system hardware components indicating the impact or classification level of the information permitted to be processed, stored or transmitted by the hardware component.	5	
ISM-1730	N/A	A software bill of materials is produced and made available to consumers of software.				Functional	equal	Software Bill of Materials (SBOM)	TDA-04.2	Mechanisms exist to generate, or obtain, a Software Bill of Materials (SBOM) for systems, applications and services that lists software packages in use, including versions and applicable licenses.	10	
ISM-1731	N/A	Planning and coordination of intrusion remediation activities are conducted on a separate system to that which has been compromised.				Functional	subset of	Chain of Custody & Forensics	IRO-08	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	Essential 8 ML1	Essential 8 ML1	Essential 8 ML1	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
ISM-1732	N/A	To the extent possible, all intrusion remediation activities are conducted in a coordinated manner during the same planned outage.				Functional	subset of	Chain of Custody & Forensics	IRO-08	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	10	
ISM-1735	N/A	Faulty or damaged media that cannot be successfully sanitised is destroyed prior to its disposal.				Functional	subset of	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	10	
ISM-1736	N/A	A managed service register is developed, implemented, maintained and verified on a regular basis.				Functional	equal	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's systems, applications, services and data.	10	
ISM-1737	N/A	A managed service register contains the following for each managed service: - the managed service provider's name - the managed service's name - the purpose for using the managed service - the sensitivity or classification of data involved - the due date for the next security assessment of the managed service - the contractual arrangements for the managed service - the point of contact for users of the managed service - the 24/7 contact details for the managed service provider.				Functional	subset of	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's systems, applications, services and data.	10	
ISM-1738	N/A	The right to verify compliance with security requirements documented in contractual arrangements with service providers is exercised on a regular and ongoing basis.				Functional	subset of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	10	
ISM-1739	N/A	A system's security architecture is approved prior to the development of the system.				Functional	intersects with	Cybersecurity & Data Privacy In Project Management	PRM-04	Mechanisms exist to assess cybersecurity & data privacy controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.	5	
ISM-1739	N/A	A system's security architecture is approved prior to the development of the system.				Functional	intersects with	Cybersecurity & Data Privacy Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical systems, system components or services at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
ISM-1739	N/A	A system's security architecture is approved prior to the development of the system.				Functional	intersects with	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to systems within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
ISM-1739	N/A	A system's security architecture is approved prior to the development of the system.				Functional	subset of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	10	
ISM-1739	N/A	A system's security architecture is approved prior to the development of the system.				Functional	intersects with	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for cybersecurity & data privacy principles that addresses risk to organizational operations, assets, individuals, other organizations.	5	
ISM-1739	N/A	A system's security architecture is approved prior to the development of the system.				Functional	intersects with	Defense-In-Depth (DiD) Architecture	SEA-03	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	5	
ISM-1740	N/A	Personnel dealing with banking details and payment requests are advised of what business email compromise is, how to manage such situations and how to report it.				Functional	intersects with	Cybersecurity & Data Privacy Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	
ISM-1740	N/A	Personnel dealing with banking details and payment requests are advised of what business email compromise is, how to manage such situations and how to report it.				Functional	intersects with	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
ISM-1740	N/A	Personnel dealing with banking details and payment requests are advised of what business email compromise is, how to manage such situations and how to report it.				Functional	intersects with	Suspicious Communications & Anomalous System Behavior	SAT-03.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.	5	
ISM-1741	N/A	IT equipment destruction processes, and supporting IT equipment destruction procedures, are developed, implemented and maintained.				Functional	subset of	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	10	
ISM-1742	N/A	IT equipment that cannot be sanitised is destroyed.				Functional	subset of	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	10	
ISM-1743	N/A	Operating systems are chosen from vendors that have demonstrated a commitment to secure-by-design and secure-by- default principles, use of memory-safe programming languages where possible, secure programming practices, and maintaining the security of their products.				Functional	subset of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	10	
ISM-1743	N/A	Operating systems are chosen from vendors that have demonstrated a commitment to secure-by-design and secure-by- default principles, use of memory-safe programming languages where possible, secure programming practices, and maintaining the security of their products.				Functional	intersects with	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for cybersecurity & data privacy principles that addresses risk to organizational operations, assets, individuals, other organizations.	5	
ISM-1743	N/A	Operating systems are chosen from vendors that have demonstrated a commitment to secure-by-design and secure-by- default principles, use of memory-safe programming languages where possible, secure programming practices, and maintaining the security of their products.				Functional	intersects with	Defense-In-Depth (DiD) Architecture	SEA-03	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	5	
ISM-1743	N/A	Operating systems are chosen from vendors that have demonstrated a commitment to secure-by-design and secure-by- default principles, use of memory-safe programming languages where possible, secure programming practices, and maintaining the security of their products.				Functional	intersects with	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique systems, system components or services.	5	
ISM-1745	N/A	Early Launch Antimalware, Secure Boot, Trusted Boot and Measured Boot functionality is enabled.				Functional	subset of	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	10	
ISM-1746	N/A	When implementing application control using path rules, only approved users can change file system permissions for approved files and folders.				Functional	subset of	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	10	
ISM-1748	N/A	Email client security settings cannot be changed by users.				Functional	subset of	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	10	
ISM-1749	N/A	Cached credentials are limited to one previous logon.				Functional	intersects with	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	5	
ISM-1749	N/A	Cached credentials are limited to one previous logon.				Functional	intersects with	Protection of Authenticators	IAC-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	5	
ISM-1750	N/A	Administrative infrastructure for critical servers, high-value servers and regular servers is segregated from each other.				Functional	intersects with	Cloud Infrastructure Security Subnet	CLD-03	Mechanisms exist to host security-specific technologies in a dedicated subnet.	5	
ISM-1750	N/A	Administrative infrastructure for critical servers, high-value servers and regular servers is segregated from each other.				Functional	intersects with	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	5	
ISM-1750	N/A	Administrative infrastructure for critical servers, high-value servers and regular servers is segregated from each other.				Functional	intersects with	Security Management Subnets	NET-06.1	Mechanisms exist to implement security management subnets to isolate security tools and support components from other internal system components by implementing separate subnetworks with managed interfaces to other components of the system.	5	
ISM-1751	N/A	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of IT equipment other than workstations, servers and network devices are applied within one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.				Functional	subset of	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	10	
ISM-1752	N/A	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in operating systems of IT equipment other than workstations, servers and network devices.				Functional	subset of	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	10	
ISM-1753	N/A	Network devices and other IT equipment that are no longer supported by vendors are replaced.				Functional	subset of	Unsupported Systems	TDA-17	Mechanisms exist to prevent unsupported systems by: (1) Replacing systems 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 system components required to satisfy mission/business needs.	10	
ISM-1754	N/A	Vulnerabilities identified in applications are resolved by software developers in a timely manner.				Functional	subset of	Cybersecurity & Data Privacy Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with cybersecurity & data privacy personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and (3) Document the results of the security testing/evaluation and flaw remediation processes.	10	
ISM-1755	N/A	A vulnerability disclosure policy is developed, implemented and maintained.				Functional	equal	Vulnerability Disclosure Program (VDP)	THR-06	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of products and services that receives unsolicited input from the public about vulnerabilities in organizational systems, services and processes.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	Essential 8 ML1	Essential 8 ML1	Essential 8 ML1	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
ISM-1756	N/A	Vulnerability disclosure processes, and supporting vulnerability disclosure procedures, are developed, implemented and maintained.				Functional	subset of	Vulnerability Disclosure Program (VDP)	THR-06	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of products and services that receives unsolicited input from the public about vulnerabilities in organizational systems, services and processes.	10	
ISM-1759	N/A	When using DH for agreeing on encryption session keys, a modulus of at least 3072 bits is used, preferably 3072 bits.				Functional	subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
ISM-1761	N/A	When using ECDH for agreeing on encryption session keys, NIST P-256, P-384 or P-521 curves are used, preferably the NIST P-384 curve.				Functional	subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
ISM-1762	N/A	When using ECDH for agreeing on encryption session keys, NIST P-384 or P-521 curves are used, preferably the NIST P-384 curve.				Functional	subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
ISM-1763	N/A	When using ECDSA for digital signatures, NIST P-256, P-384 or P-521 curves are used, preferably the NIST P-384 curve.				Functional	subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
ISM-1764	N/A	When using ECDSA for digital signatures, NIST P-384 or P-521 curves are used, preferably the NIST P-384 curve.				Functional	subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
ISM-1765	N/A	When using RSA for digital signatures, and passing encryption session keys or similar keys, a modulus of at least 3072 bits is used, preferably 3072 bits.				Functional	subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
ISM-1766	N/A	When using SHA-2 for hashing, an output size of at least 224 bits is used, preferably SHA-384.				Functional	subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
ISM-1767	N/A	When using SHA-2 for hashing, an output size of at least 256 bits is used, preferably SHA-384.				Functional	subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
ISM-1768	N/A	When using SHA-2 for hashing, an output size of at least 384 bits is used, preferably SHA-384.				Functional	subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
ISM-1769	N/A	When using AES for encryption, AES-128, AES-192 or AES-256 is used, preferably AES-256.				Functional	subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
ISM-1770	N/A	When using AES for encryption, AES-192 or AES-256 is used, preferably AES-256.				Functional	subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
ISM-1771	N/A	AES is used for encrypting IPsec connections, preferably ENCR_AES_GCM_16.				Functional	subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
ISM-1772	N/A	PRF_HMAC_SHA2_256, PRF_HMAC_SHA2_384 or PRF_HMAC_SHA2_512 is used for IPsec connections, preferably PRF_HMAC_SHA2_512.				Functional	subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
ISM-1773	N/A	System administrators for gateways that connect to Australian Government Access Only networks are Australian nationals or seconded foreign nationals.				Functional	subset of	Citizenship Requirements	HRS-04.3	Mechanisms exist to verify that individuals accessing a system processing, storing, or transmitting sensitive information meet applicable statutory, regulatory and/or contractual requirements for citizenship.	10	
ISM-1774	N/A	Gateways are managed via a secure path isolated from all connected networks.				Functional	subset of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
ISM-1778	N/A	When manually importing data to systems, all data that fails security checks is quarantined until reviewed and subsequently approved or not approved for release.				Functional	intersects with	Ad-Hoc Transfers	DCH-17	Mechanisms exist to secure ad-hoc exchanges of large digital files with internal or external parties.	5	
ISM-1778	N/A	When manually importing data to systems, all data that fails security checks is quarantined until reviewed and subsequently approved or not approved for release.				Functional	intersects with	Resource Containment	NET-08.4	Automated mechanisms exist to enforce resource containment protections that remove or quarantine a resource's access to other resources.	5	
ISM-1779	N/A	When manually exporting data from systems, all data that fails security checks is quarantined until reviewed and subsequently approved or not approved for release.				Functional	intersects with	Ad-Hoc Transfers	DCH-17	Mechanisms exist to secure ad-hoc exchanges of large digital files with internal or external parties.	5	
ISM-1779	N/A	When manually exporting data from systems, all data that fails security checks is quarantined until reviewed and subsequently approved or not approved for release.				Functional	intersects with	Resource Containment	NET-08.4	Automated mechanisms exist to enforce resource containment protections that remove or quarantine a resource's access to other resources.	5	
ISM-1780	N/A	SecDevOps practices are used for application development.				Functional	intersects with	Continuing Professional Education (CPE) - DevOps Personnel	SAT-03.8	Mechanisms exist to ensure application development and operations (DevOps) personnel receive Continuing Professional Education (CPE) training on Secure Software Development Practices (SSDP) to appropriately address evolving threats.	5	
ISM-1780	N/A	SecDevOps practices are used for application development.				Functional	subset of	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10	
ISM-1781	N/A	All data communicated over network infrastructure is encrypted.				Functional	subset of	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	10	
ISM-1782	N/A	A protective DNS service is used to block access to known malicious domain names.				Functional	intersects with	Heuristic / Nonsignature-Based Detection	END-04.4	Mechanisms exist to utilize heuristic / nonsignature-based antimalware detection capabilities.	5	
ISM-1782	N/A	A protective DNS service is used to block access to known malicious domain names.				Functional	intersects with	Domain Name Service (DNS) Resolution	NET-10	Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.	5	
ISM-1783	N/A	Public IP addresses controlled by, or used by, an organisation are signed by valid ROA records.				Functional	subset of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
ISM-1784	N/A	The cyber security incident management policy, including the associated cyber security incident response plan, is exercised at least annually.				Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
ISM-1784	N/A	The cyber security incident management policy, including the associated cyber security incident response plan, is exercised at least annually.				Functional	intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
ISM-1785	N/A	A supplier relationship management policy is developed, implemented and maintained.				Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
ISM-1785	N/A	A supplier relationship management policy is developed, implemented and maintained.				Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
ISM-1785	N/A	A supplier relationship management policy is developed, implemented and maintained.				Functional	subset of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
ISM-1786	N/A	An approved supplier list is developed, implemented and maintained.				Functional	subset of	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's systems, applications, services and data.	10	
ISM-1787	N/A	Applications, IT equipment, OT equipment and services are sourced from approved suppliers				Functional	subset of	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related services.	10	
ISM-1788	N/A	Multiple potential suppliers are identified for sourcing critical applications, IT equipment, OT equipment and services.				Functional	subset of	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique systems, system components or services.	10	
ISM-1789	N/A	Sufficient spares of critical IT equipment and OT equipment are sourced and kept in reserve.				Functional	intersects with	Reserve Hardware	BCD-15	Mechanisms exist to purchase and maintain a sufficient reserve of spare hardware to ensure essential missions and business functions can be maintained in the event of a supply chain disruption.	5	
ISM-1789	N/A	Sufficient spares of critical IT equipment and OT equipment are sourced and kept in reserve.				Functional	intersects with	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with the services and product supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5	
ISM-1789	N/A	Sufficient spares of critical IT equipment and OT equipment are sourced and kept in reserve.				Functional	intersects with	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique systems, system components or services.	5	
ISM-1790	N/A	Applications, IT equipment, OT equipment and services are delivered in a manner that maintains their integrity.				Functional	intersects with	Provenance	AST-03.2	Mechanisms exist to track the origin, development, ownership, location and changes to systems, system components and associated data.	5	
ISM-1790	N/A	Applications, IT equipment, OT equipment and services are delivered in a manner that maintains their integrity.				Functional	intersects with	Product Tampering and Counterfeiting (PTC)	TDA-11	Mechanisms exist to maintain awareness of component authenticity by developing and implementing Product Tampering and Counterfeiting (PTC) practices that include the means to detect and prevent counterfeit components.	5	
ISM-1791	N/A	The integrity of applications, IT equipment, OT equipment and services are assessed as part of acceptance of products and services.				Functional	intersects with	Provenance	AST-03.2	Mechanisms exist to track the origin, development, ownership, location and changes to systems, system components and associated data.	5	
ISM-1791	N/A	The integrity of applications, IT equipment, OT equipment and services are assessed as part of acceptance of products and services.				Functional	intersects with	Product Tampering and Counterfeiting (PTC)	TDA-11	Mechanisms exist to maintain awareness of component authenticity by developing and implementing Product Tampering and Counterfeiting (PTC) practices that include the means to detect and prevent counterfeit components.	5	
ISM-1792	N/A	The authenticity of applications, IT equipment, OT equipment and services are assessed as part of acceptance of products and services.				Functional	intersects with	Provenance	AST-03.2	Mechanisms exist to track the origin, development, ownership, location and changes to systems, system components and associated data.	5	
ISM-1792	N/A	The authenticity of applications, IT equipment, OT equipment and services are assessed as part of acceptance of products and services.				Functional	intersects with	Product Tampering and Counterfeiting (PTC)	TDA-11	Mechanisms exist to maintain awareness of component authenticity by developing and implementing Product Tampering and Counterfeiting (PTC) practices that include the means to detect and prevent counterfeit components.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	Essential 8 ML1	Essential 8 ML1	Essential 8 ML1	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
ISM-1793	N/A	Managed service providers and their managed services undergo a security assessment by an IRAP assessor at least every 24 months.				Functional	intersects with	Third-Party Scope Review	TPM-05.5	Mechanisms exist to perform recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure cybersecurity & data privacy control assignments accurately reflect current business practices, compliance obligations, technologies and stakeholders.	5	
ISM-1793	N/A	Managed service providers and their managed services undergo a security assessment by an IRAP assessor at least every 24 months.				Functional	intersects with	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity & data privacy controls.	5	
ISM-1794	N/A	A minimum notification period of one month by service providers for significant changes to their own service provider arrangements is documented in contractual arrangements with service providers.				Functional	subset of	Managing Changes To Third-Party Services	TPM-10	Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business information, systems and processes that are in scope by the third-party.	10	
ISM-1795	N/A	Credentials for break glass accounts, local administrator accounts and service accounts are a minimum of 30 characters.				Functional	subset of	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	10	
ISM-1796	N/A	Files containing executable content are digitally signed as part of application development.				Functional	intersects with	Signed Components	CHG-04.2	Mechanisms exist to prevent the installation of software and firmware components without verification that the component has been digitally signed using an organization-approved certificate authority.	5	
ISM-1796	N/A	Files containing executable content are digitally signed as part of application development.				Functional	intersects with	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of products and/or services across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	5	
ISM-1797	N/A	Installers, patches and updates are digitally signed or provided with cryptographic checksums as part of application development.				Functional	subset of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of products and/or services across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
ISM-1798	N/A	Secure configuration guidance is produced as part of application development.				Functional	intersects with	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of products and/or services across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	5	
ISM-1798	N/A	Secure configuration guidance is produced as part of application development.				Functional	intersects with	Pre-Established Secure Configurations	TDA-02.4	Mechanisms exist to ensure vendors / manufacturers: (1) Deliver the system, component, or service with a pre-established, secure configuration implemented; and (2) Use the pre-established, secure configuration as the default for any subsequent system, component, or service reinstallation or upgrade.	5	
ISM-1798	N/A	Secure configuration guidance is produced as part of application development.				Functional	intersects with	Documentation Requirements	TDA-04	Mechanisms exist to obtain, protect and distribute administrator documentation for systems that describe: (1) Secure configuration, installation and operation of the system; (2) Effective use and maintenance of security features/functions; and (3) Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	5	
ISM-1798	N/A	Secure configuration guidance is produced as part of application development.				Functional	intersects with	Functional Properties	TDA-04.1	Mechanisms exist to require software developers to provide information describing the functional properties of the security controls to be utilized within systems, system components or services in sufficient detail to permit analysis and testing of the controls.	5	
ISM-1799	N/A	Incoming emails are rejected if they do not pass DMARC checks.				Functional	intersects with	Domain Name Service (DNS) Resolution	NET-10	Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.	5	
ISM-1799	N/A	Incoming emails are rejected if they do not pass DMARC checks.				Functional	intersects with	Sender Policy Framework (SPF)	NET-10.3	Mechanisms exist to validate the legitimacy of email communications through configuring a Domain Naming Service (DNS) Sender Policy Framework (SPF) record to specify the IP addresses and/or hostnames that are authorized to send email from the specified domain.	5	
ISM-1800	N/A	Network devices are flashed with trusted firmware before they are used for the first time.				Functional	subset of	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	10	
ISM-1801	N/A	Network devices are restarted on at least a monthly basis.				Functional	subset of	Continuous Vulnerability Remediation Activities	VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	10	
ISM-1802	N/A	HACE are issued an Approval for Use by ASD and operated in accordance with the latest version of their associated Australian Communications Security Instructions.				Functional	subset of	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is stored.	10	
ISM-1803	N/A	A cyber security incident register contains the following for each cyber security incident: - the date the cyber security incident occurred - the date the cyber security incident was discovered - a description of the cyber security incident - any actions taken in response to the cyber security incident - to whom the cyber security incident was reported.				Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
ISM-1803	N/A	A cyber security incident register contains the following for each cyber security incident: - the date the cyber security incident occurred - the date the cyber security incident was discovered - a description of the cyber security incident - any actions taken in response to the cyber security incident - to whom the cyber security incident was reported.				Functional	intersects with	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity & data privacy incidents to internal stakeholders all the way through the resolution of the incident.	5	
ISM-1806	N/A	Default accounts or credentials for user applications, including for any pre-configured accounts, are changed.				Functional	subset of	Default Authenticators	IAC-10.8	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	10	
ISM-1805	N/A	A denial of service response plan for video conferencing and IP telephony services contains the following: - how to identify signs of a denial-of-service attack - how to identify the source of a denial-of-service attack - how capabilities can be maintained during a denial-of-service attack - what actions can be taken to respond to a denial-of-service attack.				Functional	subset of	Denial of Service (DoS) Protection	NET-02.1	Automated mechanisms exist to protect against or limit the effects of denial of service attacks.	10	
ISM-1804	N/A	Break clauses associated with failure to meet security requirements are documented in contractual arrangements with service providers.				Functional	subset of	Break Clauses	TPM-05.7	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for cybersecurity and/or data privacy controls.	10	
ISM-1807	N/A	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.	ML1	ML2	ML3	Functional	intersects with	Asset Inventories	AST-02	Mechanisms exist to maintain a current list of approved technologies (hardware and software).	5	Essential Eight: ML1, ML2, ML3
ISM-1807	N/A	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.	ML1	ML2	ML3	Functional	intersects with	Automated Unauthorized Component Detection	AST-02.2	Mechanisms exist to maintain a current list of approved technologies (hardware and software).	5	Essential Eight: ML1, ML2, ML3
ISM-1808	N/A	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	ML1	ML2	ML3	Functional	subset of	Update Tool Capability	VPM-06.1	Mechanisms exist to update vulnerability scanning tools.	10	Essential Eight: ML1, ML2, ML3
ISM-1809	N/A	When applications, operating systems, network devices or other IT equipment that are no longer supported by vendors cannot be immediately removed or replaced, compensating controls are implemented until such time that they can be removed or replaced.				Functional	subset of	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	10	
ISM-1810	N/A	Backups of data, applications and settings are synchronised to enable restoration to a common point in time.	ML1	ML2	ML3	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	Essential Eight: ML1, ML2, ML3
ISM-1810	N/A	Backups of data, applications and settings are synchronised to enable restoration to a common point in time.	ML1	ML2	ML3	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 satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	Essential Eight: ML1, ML2, ML3
ISM-1811	N/A	Backups of data, applications and settings are retained in a secure and resilient manner.	ML1	ML2	ML3	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 satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	Essential Eight: ML1, ML2, ML3
ISM-1811	N/A	Backups of data, applications and settings are retained in a secure and resilient manner.	ML1	ML2	ML3	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	Essential Eight: ML1, ML2, ML3
ISM-1812	N/A	Unprivileged accounts cannot access backups belonging to other accounts.	ML1	ML2	ML3	Functional	equal	Backup Access	BCD-11.9	Mechanisms exist to restrict access to backups to privileged users with assigned roles for data backup and recovery operations.	10	Essential Eight: ML1, ML2, ML3
ISM-1813	N/A	Unprivileged accounts cannot access their own backups.			ML3	Functional	equal	Backup Access	BCD-11.9	Mechanisms exist to restrict access to backups to privileged users with assigned roles for data backup and recovery operations.	10	Essential Eight: ML3

FDE #	FDE Name	Focal Document Element (FDE) Description	Essential 8 ML1	Essential 8 ML1	Essential 8 ML1	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
ISM-1814	N/A	Unprivileged accounts are prevented from modifying and deleting backups.	ML1	ML2	ML3	Functional	equal	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.	10	Essential Eight: ML1, ML2, ML3
ISM-1815	N/A	Event logs are protected from unauthorised modification and deletion.		ML2	ML3	Functional	equal	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	10	Essential Eight: ML2, ML3
ISM-1816	N/A	Unauthorised modification of the authoritative source for software is prevented.				Functional	subset of	Access to Program Source Code	TDA-20	Mechanisms exist to limit privileges to change software resident within software libraries.	10	
ISM-1817	N/A	Authentication and authorisation of clients is performed when clients call web APIs that facilitate access to data not authorised for release into the public domain.				Functional	subset of	Application & Program Interface (API) Security	CLD-04	Mechanisms exist to ensure support for secure interoperability between components with Application & Program Interfaces (APIs).	10	
ISM-1818	N/A	Authentication and authorisation of clients is performed when clients call web APIs that facilitate modification of data.				Functional	subset of	Application & Program Interface (API) Security	CLD-04	Mechanisms exist to ensure support for secure interoperability between components with Application & Program Interfaces (APIs).	10	
ISM-1819	N/A	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.		ML2	ML3	Functional	subset of	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	10	Essential Eight: ML2, ML3
ISM-1820	N/A	Cables for individual systems use a consistent colour.				Functional	subset of	Component Marking	PES-16	Physical security mechanisms exist to mark system hardware components indicating the impact or classification level of the information permitted to be processed, stored or transmitted by the hardware component.	10	
ISM-1821	N/A	TOP SECRET cables, when bundled together or run in conduit, are run exclusively in their own individual cable bundle or conduit.				Functional	subset of	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
ISM-1822	N/A	Wall outlet boxes for individual systems use a consistent colour.				Functional	subset of	Component Marking	PES-16	Physical security mechanisms exist to mark system hardware components indicating the impact or classification level of the information permitted to be processed, stored or transmitted by the hardware component.	10	
ISM-1823	N/A	Office productivity suite security settings cannot be changed by users.		ML2	ML3	Functional	intersects with	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.	5	Essential Eight: ML2, ML3
ISM-1823	N/A	Office productivity suite security settings cannot be changed by users.		ML2	ML3	Functional	intersects with	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	Essential Eight: ML2, ML3
ISM-1824	N/A	PDF software security settings cannot be changed by users.		ML2	ML3	Functional	intersects with	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.	5	Essential Eight: ML2, ML3
ISM-1824	N/A	PDF software security settings cannot be changed by users.		ML2	ML3	Functional	intersects with	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	Essential Eight: ML2, ML3
ISM-1825	N/A	Security product security settings cannot be changed by users.				Functional	intersects with	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.	5	
ISM-1825	N/A	Security product security settings cannot be changed by users.				Functional	intersects with	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
ISM-1826	N/A	Server applications are chosen from vendors that have demonstrated a commitment to secure-by-design and secure-by- default principles, use of memory-safe programming languages where possible, secure programming practices, and maintaining the security of their products.				Functional	intersects with	Development Methods, Techniques & Processes	TDA-02.3	Mechanisms exist to require software developers to ensure that their software development processes employ industry-recognized secure practices for secure programming, engineering methods, quality control processes and validation techniques to minimize flawed and/or malformed software.	5	
ISM-1826	N/A	Server applications are chosen from vendors that have demonstrated a commitment to secure-by-design and secure-by- default principles, use of memory-safe programming languages where possible, secure programming practices, and maintaining the security of their products.				Functional	intersects with	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5	
ISM-1826	N/A	Server applications are chosen from vendors that have demonstrated a commitment to secure-by-design and secure-by- default principles, use of memory-safe programming languages where possible, secure programming practices, and maintaining the security of their products.				Functional	intersects with	Secure Settings By Default	TDA-09.6	Mechanisms exist to implement secure configuration settings by default to reduce the likelihood of software being deployed with weak security settings that would put the asset at a greater risk of compromise.	5	
ISM-1827	N/A	Microsoft AD DS domain controllers are administered using dedicated domain administrator user accounts that are not used to administer other systems.				Functional	intersects with	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.	5	
ISM-1827	N/A	Microsoft AD DS domain controllers are administered using dedicated domain administrator user accounts that are not used to administer other systems.				Functional	intersects with	Privileged Account Separation	IAC-16.2	Mechanisms exist to separate privileged accounts between infrastructure environments to reduce the risk of a compromise in one infrastructure environment from laterally affecting other infrastructure environments.	5	
ISM-1828	N/A	The Print Spooler service is disabled on Microsoft AD DS domain controllers.				Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
ISM-1828	N/A	The Print Spooler service is disabled on Microsoft AD DS domain controllers.				Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
ISM-1829	N/A	Passwords and cpasswords are not used in Group Policy Preferences.				Functional	subset of	Baseline Tailoring	CFG-02.9	Mechanisms exist to allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to: (1) Mission / business functions; (2) Operational environment; (3) Specific threats or vulnerabilities; or (4) Other conditions or situations that could affect mission / business success.	10	
ISM-1830	N/A	Security-related events for Microsoft AD DS are centrally logged.				Functional	subset of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
ISM-1830	N/A	Security-related events for Microsoft AD DS are centrally logged.				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-1830	N/A	Security-related events for Microsoft AD DS are centrally logged.				Functional	intersects with	Event Log Retention	MON-10	Mechanisms exist to retain event logs for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	5	
ISM-1832	N/A	Only service accounts and computer accounts are configured with Service Principal Names (SPNs).				Functional	intersects with	Dedicated Administrative Machines	IAC-20.4	Mechanisms exist to restrict executing administrative tasks or tasks requiring elevated access to a dedicated machine.	5	
ISM-1832	N/A	Only service accounts and computer accounts are configured with Service Principal Names (SPNs).				Functional	intersects with	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	5	
ISM-1832	N/A	Only service accounts and computer accounts are configured with Service Principal Names (SPNs).				Functional	intersects with	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
ISM-1833	N/A	Service accounts are provisioned with the minimum privileges required and are not members of the domain administrators group or similar highly privileged groups.				Functional	intersects with	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	5	
ISM-1833	N/A	Service accounts are provisioned with the minimum privileges required and are not members of the domain administrators group or similar highly privileged groups.				Functional	intersects with	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
ISM-1834	N/A	Duplicate SPNs do not exist within the domain.				Functional	subset of	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	10	
ISM-1835	N/A	Privileged user accounts are configured as sensitive and cannot be delegated.				Functional	intersects with	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	5	
ISM-1835	N/A	Privileged user accounts are configured as sensitive and cannot be delegated.				Functional	intersects with	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.	5	
ISM-1837	N/A	User accounts are not configured with password never expires or password not required.				Functional	subset of	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	10	
ISM-1836	N/A	User accounts require Kerberos pre-authentication.				Functional	subset of	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	10	
ISM-1838	N/A	The UserPassword attribute for user accounts is not used.				Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
ISM-1838	N/A	The UserPassword attribute for user accounts is not used.				Functional	intersects with	Baseline Tailoring	CFG-02.9	Mechanisms exist to allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to: (1) Mission / business functions; (2) Operational environment; (3) Specific threats or vulnerabilities; or (4) Other conditions or situations that could affect mission / business success.	5	
ISM-1839	N/A	Account properties accessible by unprivileged users are not used to store passwords.				Functional	subset of	Baseline Tailoring	CFG-02.9	Mechanisms exist to allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to: (1) Mission / business functions; (2) Operational environment; (3) Specific threats or vulnerabilities; or (4) Other conditions or situations that could affect mission / business success.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	Essential 8 ML1	Essential 8 ML1	Essential 8 ML1	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
ISM-1840	N/A	User account passwords do not use reversible encryption.				Functional	intersects with	Baseline Tailoring	CFG-02.9	Mechanisms exist to allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to: (1) Mission / business functions; (2) Operational environment; (3) Specific threats or vulnerabilities; or (4) Other conditions or situations that could affect mission / business success.	5	
ISM-1840	N/A	User account passwords do not use reversible encryption.				Functional	intersects with	Baseline Tailoring	CFG-02.9	Mechanisms exist to allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to: (1) Mission / business functions; (2) Operational environment; (3) Specific threats or vulnerabilities; or (4) Other conditions or situations that could affect mission / business success.	5	
ISM-1841	N/A	Unprivileged user accounts cannot add machines to the domain.				Functional	intersects with	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
ISM-1841	N/A	Unprivileged user accounts cannot add machines to the domain.				Functional	intersects with	Prohibit Non-Privileged Users from Executing Privileged Functions	IAC-21.5	Mechanisms exist to prevent non-privileged users from executing privileged functions to include disabling, circumventing or altering implemented security safeguards / countermeasures.	5	
ISM-1842	N/A	Dedicated service accounts are used to add machines to the domain.				Functional	intersects with	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
ISM-1842	N/A	Dedicated service accounts are used to add machines to the domain.				Functional	intersects with	Authorize Access to Security Functions	IAC-21.1	Mechanisms exist to limit access to security functions to explicitly-authorized privileged users.	5	
ISM-1842	N/A	Dedicated service accounts are used to add machines to the domain.				Functional	intersects with	Privileged Accounts	IAC-21.3	Mechanisms exist to restrict the assignment of privileged accounts to management-approved personnel and/or roles.	5	
ISM-1843	N/A	User accounts with unconstrained delegation are reviewed at least annually, and those without an associated Kerberos SPN or demonstrated business requirement are removed.				Functional	intersects with	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	5	
ISM-1843	N/A	User accounts with unconstrained delegation are reviewed at least annually, and those without an associated Kerberos SPN or demonstrated business requirement are removed.				Functional	intersects with	System Account Reviews	IAC-15.7	Mechanisms exist to review all system accounts and disable any account that cannot be associated with a business process and owner.	5	
ISM-1844	N/A	Computer accounts that are not Microsoft AD DS domain controllers are not trusted for delegation to services.				Functional	subset of	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	10	
ISM-1845	N/A	When a user account is disabled, it is removed from all security group memberships.				Functional	subset of	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	10	
ISM-1846	N/A	The Pre-Windows 2000 Compatible Access security group does not contain user accounts.				Functional	subset of	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	10	
ISM-1847	N/A	Credentials for the Kerberos Key Distribution Center's service account (KRBTGT) are changed twice, allowing for replication to all Microsoft Active Directory Domain Services domain controllers in-between each change, if: - the domain has been directly compromised - the domain is suspected of being compromised - they have not been changed in the past 12 months.				Functional	subset of	Federated Credential Management	IAC-13.2	Mechanisms exist to federate credentials to allow cross-organization authentication of individuals and devices.	10	
ISM-1848	N/A	When using a software-based isolation mechanism to share a physical server's hardware, the isolation mechanism or underlying operating system is replaced when it is no longer supported by a vendor.				Functional	subset of	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and upgrades.	10	
ISM-1849	N/A	The OWASP Top 10 Proactive Controls are used in the development of web applications.				Functional	subset of	Development Methods, Techniques & Processes	TDA-02.3	Mechanisms exist to require software developers to ensure that their software development processes employ industry-recognized secure practices for secure programming, engineering methods, quality control processes and validation techniques to minimize flawed and/or malformed software.	10	
ISM-1850	N/A	The OWASP Top 10 are mitigated in the development of web applications.				Functional	subset of	Development Methods, Techniques & Processes	TDA-02.3	Mechanisms exist to require software developers to ensure that their software development processes employ industry-recognized secure practices for secure programming, engineering methods, quality control processes and validation techniques to minimize flawed and/or malformed software.	10	
ISM-1851	N/A	The OWASP API Security Top 10 are mitigated in the development of web APIs.				Functional	subset of	Development Methods, Techniques & Processes	TDA-02.3	Mechanisms exist to require software developers to ensure that their software development processes employ industry-recognized secure practices for secure programming, engineering methods, quality control processes and validation techniques to minimize flawed and/or malformed software.	10	
ISM-1852	N/A	Unprivileged access to systems, applications and data repositories is limited to only what is required for users and services to undertake their duties.				Functional	subset of	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	10	
ISM-1854	N/A	Users authenticate to MFDs before they can print, scan or copy documents.				Functional	intersects with	Multi-Function Devices (MFD)	AST-23	Mechanisms exist to securely configure Multi-Function Devices (MFD) according to industry-recognized secure practices for the type of device.	5	
ISM-1854	N/A	Users authenticate to MFDs before they can print, scan or copy documents.				Functional	intersects with	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
ISM-1855	N/A	Use of MFDs for printing, scanning and copying purposes, including the capture of shadow copies of documents, are centrally logged.				Functional	intersects with	Multi-Function Devices (MFD)	AST-23	Mechanisms exist to securely configure Multi-Function Devices (MFD) according to industry-recognized secure practices for the type of device.	5	
ISM-1855	N/A	Use of MFDs for printing, scanning and copying purposes, including the capture of shadow copies of documents, are centrally logged.				Functional	intersects with	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	
ISM-1857	N/A	IT equipment is chosen from vendors that have demonstrated a commitment to secure-by-design and secure-by-default principles, use of memory-safe programming languages where possible, secure programming practices, and maintaining the security of their products.				Functional	subset of	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	10	
ISM-1858	N/A	IT equipment is hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.				Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
ISM-1858	N/A	IT equipment is hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.				Functional	intersects with	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	5	
ISM-1859	N/A	Office productivity suites are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.		ML2	ML3	Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	Essential Eight: ML2, ML3
ISM-1859	N/A	Office productivity suites are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.		ML2	ML3	Functional	intersects with	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	5	Essential Eight: ML2, ML3
ISM-1860	N/A	PDF software is hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.		ML2	ML3	Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	Essential Eight: ML2, ML3
ISM-1860	N/A	PDF software is hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.		ML2	ML3	Functional	intersects with	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	5	Essential Eight: ML2, ML3
ISM-1861	N/A	Local Security Authority protection functionality is enabled.			ML3	Functional	subset of	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	10	Essential Eight: ML3
ISM-1862	N/A	If using a WAF, disclosing the IP addresses of web servers under an organisation's control (referred to as origin servers) is avoided and access to the origin servers is restricted to the WAF and authorised management networks.				Functional	subset of	Web Application Firewall (WAF)	WEB-03	Mechanisms exist to deploy Web Application Firewalls (WAFs) to provide defense-in-depth protection for application-specific threats.	10	
ISM-1863	N/A	Networked management interfaces for IT equipment are not directly exposed to the internet.				Functional	intersects with	Layered Network Defenses	NET-02	Mechanisms exist to implement security functions as a layered structure that minimizes interactions between layers of the design and avoids any dependence by lower layers on the functionality or correctness of higher layers.	5	
ISM-1863	N/A	Networked management interfaces for IT equipment are not directly exposed to the internet.				Functional	intersects with	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
ISM-1863	N/A	Networked management interfaces for IT equipment are not directly exposed to the internet.				Functional	intersects with	Direct Internet Access Restrictions	NET-06.4	Mechanisms exist to prohibit, or strictly-control, Internet access from sensitive / regulated data enclaves (secure zones).	5	
ISM-1863	N/A	Networked management interfaces for IT equipment are not directly exposed to the internet.				Functional	intersects with	Use of Demilitarized Zones (DMZ)	WEB-02	Mechanisms exist to utilize a Demilitarized Zone (DMZ) to restrict inbound traffic to authorized devices on certain services, protocols and ports.	5	
ISM-1864	N/A	A system usage policy is developed, implemented and maintained.				Functional	intersects with	Usage Parameters	AST-14	Mechanisms exist to monitor and enforce usage parameters that limit the potential damage caused from the unauthorized or unintentional alteration of system parameters.	5	
ISM-1864	N/A	A system usage policy is developed, implemented and maintained.				Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
ISM-1865	N/A	Personnel agree to abide by usage policies associated with a system and its resources before being granted access to the system and its resources.				Functional	intersects with	Usage Parameters	AST-14	Mechanisms exist to monitor and enforce usage parameters that limit the potential damage caused from the unauthorized or unintentional alteration of system parameters.	5	
ISM-1865	N/A	Personnel agree to abide by usage policies associated with a system and its resources before being granted access to the system and its resources.				Functional	intersects with	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity & data privacy principles in their daily work.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	Essential 8 ML1	Essential 8 ML1	Essential 8 ML1	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
ISM-1866	N/A	Personnel accessing OFFICIAL: Sensitive or PROTECTED systems or data using privately-owned mobile devices or desktop computers are prevented from storing classified data on their privately-owned mobile devices and desktop computers.				Functional	intersects with	Use of Personal Devices	AST-12	Mechanisms exist to restrict the possession and usage of personally-owned technology devices within organization-controlled facilities.	5	
ISM-1866	N/A	Personnel accessing OFFICIAL: Sensitive or PROTECTED systems or data using privately-owned mobile devices or desktop computers are prevented from storing classified data on their privately-owned mobile devices and desktop computers.				Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
ISM-1866	N/A	Personnel accessing OFFICIAL: Sensitive or PROTECTED systems or data using privately-owned mobile devices or desktop computers are prevented from storing classified data on their privately-owned mobile devices and desktop computers.				Functional	intersects with	Portable Storage Devices	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.	5	
ISM-1866	N/A	Personnel accessing OFFICIAL: Sensitive or PROTECTED systems or data using privately-owned mobile devices or desktop computers are prevented from storing classified data on their privately-owned mobile devices and desktop computers.				Functional	intersects with	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
ISM-1867	N/A	Mobile devices that access OFFICIAL: Sensitive or PROTECTED systems or data use mobile platforms that have completed a Common Criteria evaluation against the Protection Profile for Mobile Device Fundamentals, version 3.3 or later, and are operated in accordance with the latest version of their associated ASD security configuration guide.				Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
ISM-1867	N/A	Mobile devices that access OFFICIAL: Sensitive or PROTECTED systems or data use mobile platforms that have completed a Common Criteria evaluation against the Protection Profile for Mobile Device Fundamentals, version 3.3 or later, and are operated in accordance with the latest version of their associated ASD security configuration guide.				Functional	intersects with	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
ISM-1867	N/A	Mobile devices that access OFFICIAL: Sensitive or PROTECTED systems or data use mobile platforms that have completed a Common Criteria evaluation against the Protection Profile for Mobile Device Fundamentals, version 3.3 or later, and are operated in accordance with the latest version of their associated ASD security configuration guide.				Functional	intersects with	Secure Practices Guidelines	OPS-05	Mechanisms exist to provide guidelines and recommendations for the secure use of products and/or services to assist in the configuration, installation and use of the product and/or service.	5	
ISM-1868	N/A	SECRET and TOP SECRET mobile devices do not use removable media unless approved beforehand by ASD.				Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
ISM-1868	N/A	SECRET and TOP SECRET mobile devices do not use removable media unless approved beforehand by ASD.				Functional	intersects with	Portable Storage Devices	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.	5	
ISM-1869	N/A	A non-networked IT equipment register is developed, implemented, maintained and verified on a regular basis.				Functional	subset of	Asset Inventories	AST-02	Mechanisms exist to maintain a current list of approved technologies (hardware and software).	10	
ISM-1870	N/A	Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients.	ML1	ML2	ML3	Functional	intersects with	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5	Essential Eight: ML1, ML2, ML3
ISM-1870	N/A	Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients.	ML1	ML2	ML3	Functional	intersects with	Configuration Enforcement	CFG-06	Automated mechanisms exist to monitor, enforce and report on configurations for endpoint devices.	5	Essential Eight: ML1, ML2, ML3
ISM-1870	N/A	Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients.	ML1	ML2	ML3	Functional	intersects with	Integrity Assurance & Enforcement (IAE)	CFG-06.1	Automated mechanisms exist to identify unauthorized deviations from an approved baseline and implement automated resiliency actions to remediate the unauthorized change.	5	Essential Eight: ML1, ML2, ML3
ISM-1871	N/A	Application control is applied to all locations other than user profiles and temporary folders used by operating systems, web browsers and email clients.		ML2	ML3	Functional	intersects with	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5	Essential Eight: ML2, ML3
ISM-1871	N/A	Application control is applied to all locations other than user profiles and temporary folders used by operating systems, web browsers and email clients.		ML2	ML3	Functional	intersects with	Configuration Enforcement	CFG-06	Automated mechanisms exist to monitor, enforce and report on configurations for endpoint devices.	5	Essential Eight: ML2, ML3
ISM-1871	N/A	Application control is applied to all locations other than user profiles and temporary folders used by operating systems, web browsers and email clients.		ML2	ML3	Functional	intersects with	Integrity Assurance & Enforcement (IAE)	CFG-06.1	Automated mechanisms exist to identify unauthorized deviations from an approved baseline and implement automated resiliency actions to remediate the unauthorized change.	5	Essential Eight: ML2, ML3
ISM-1872	N/A	Multi-factor authentication used for authenticating users of online services is phishing-resistant.		ML2	ML3	Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	Essential Eight: ML2, ML3
ISM-1872	N/A	Multi-factor authentication used for authenticating users of online services is phishing-resistant.		ML2	ML3	Functional	intersects with	Phishing & Spam Protection	END-08	Mechanisms exist to utilize anti-phishing and spam protection technologies to detect and take action on unsolicited messages transported by electronic mail.	5	Essential Eight: ML2, ML3
ISM-1872	N/A	Multi-factor authentication used for authenticating users of online services is phishing-resistant.		ML2	ML3	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 systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	5	Essential Eight: ML2, ML3
ISM-1873	N/A	Multi-factor authentication used for authenticating customers of online customer services provides a phishing-resistant option.		ML2		Functional	intersects with	Phishing & Spam Protection	END-08	Mechanisms exist to utilize anti-phishing and spam protection technologies to detect and take action on unsolicited messages transported by electronic mail.	5	Essential Eight: ML2
ISM-1873	N/A	Multi-factor authentication used for authenticating customers of online customer services provides a phishing-resistant option.		ML2		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 systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	5	Essential Eight: ML2
ISM-1874	N/A	Multi-factor authentication used for authenticating customers of online customer services is phishing-resistant.			ML3	Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	Essential Eight: ML3
ISM-1874	N/A	Multi-factor authentication used for authenticating customers of online customer services is phishing-resistant.			ML3	Functional	intersects with	Phishing & Spam Protection	END-08	Mechanisms exist to utilize anti-phishing and spam protection technologies to detect and take action on unsolicited messages transported by electronic mail.	5	Essential Eight: ML3
ISM-1874	N/A	Multi-factor authentication used for authenticating customers of online customer services is phishing-resistant.			ML3	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 systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	5	Essential Eight: ML3
ISM-1875	N/A	Networks are scanned at least monthly to identify any credentials that are being stored in the clear.				Functional	subset of	Integration of Scanning & Other Monitoring Information	MON-02.3	Automated mechanisms exist to integrate the analysis of audit records with analysis of vulnerability scanners, network performance, system monitoring and other sources to further enhance the ability to identify inappropriate or unusual activity.	10	
ISM-1876	N/A	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.	ML1	ML2	ML3	Functional	subset of	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	10	Essential Eight: ML1, ML2, ML3
ISM-1877	N/A	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.	ML1	ML2	ML3	Functional	subset of	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	10	Essential Eight: ML1, ML2, ML3
ISM-1878	N/A	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of IT equipment other than workstations, servers and network devices are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.				Functional	subset of	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	10	
ISM-1879	N/A	Patches, updates or other vendor mitigations for vulnerabilities in drivers are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.			ML3	Functional	subset of	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	10	Essential Eight: ML3
ISM-1880	N/A	Cyber security incidents that involve customer data are reported to customers and the public in a timely manner after they occur or are discovered.				Functional	intersects with	Cybersecurity & Data Privacy Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	5	
ISM-1880	N/A	Cyber security incidents that involve customer data are reported to customers and the public in a timely manner after they occur or are discovered.				Functional	intersects with	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.	5	
ISM-1881	N/A	Cyber security incidents that do not involve customer data are reported to customers and the public in a timely manner after they occur or are discovered.				Functional	intersects with	Cybersecurity & Data Privacy Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	5	
ISM-1881	N/A	Cyber security incidents that do not involve customer data are reported to customers and the public in a timely manner after they occur or are discovered.				Functional	intersects with	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.	5	
ISM-1882	N/A	Applications, IT equipment, OT equipment and services are chosen from suppliers that have demonstrated a commitment to transparency for their products and services.				Functional	subset of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
ISM-1882	N/A	Applications, IT equipment, OT equipment and services are chosen from suppliers that have demonstrated a commitment to transparency for their products and services.				Functional	intersects with	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with the services and product supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5	
ISM-1883	N/A	Privileged accounts explicitly authorised to access online services are strictly limited to only what is required for users and services to undertake their duties.	ML1	ML2	ML3	Functional	intersects with	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.	5	Essential Eight: ML1, ML2, ML3
ISM-1883	N/A	Privileged accounts explicitly authorised to access online services are strictly limited to only what is required for users and services to undertake their duties.	ML1	ML2	ML3	Functional	intersects with	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	Essential Eight: ML1, ML2, ML3
ISM-1884	N/A	Emanation security doctrine produced by ASD for the management of emanation security matters is complied with.				Functional	subset of	Secure Practices Guidelines	OPS-05	Mechanisms exist to provide guidelines and recommendations for the secure use of products and/or services to assist in the configuration, installation and use of the product and/or service.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	Essential 8 ML1	Essential 8 ML1	Essential 8 ML1	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
ISM-1885	N/A	Recommended actions contained within TEMPEST requirements statements issued for systems are implemented by system owners.				Functional	subset of	Secure Practices Guidelines	OPS-05	Mechanisms exist to provide guidelines and recommendations for the secure use of products and/or services to assist in the configuration, installation and use of the product and/or service.	10	
ISM-1886	N/A	Mobile devices are configured to operate in a supervised (or equivalent) mode.				Functional	subset of	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	10	
ISM-1887	N/A	Mobile devices are configured with remote locate and wipe functionality.				Functional	subset of	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	10	
ISM-1888	N/A	Mobile devices are configured with secure lock screens.				Functional	subset of	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	10	
ISM-1889	N/A	Command line process creation events are centrally logged.		ML2	ML3	Functional	subset of	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	10	Essential Eight: ML2, ML3
ISM-1890	N/A	Microsoft Office macros are checked to ensure they are free of malicious code before being digitally signed or placed within Trusted Locations.			ML3	Functional	intersects with	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	Essential Eight: ML3
ISM-1890	N/A	Microsoft Office macros are checked to ensure they are free of malicious code before being digitally signed or placed within Trusted Locations.			ML3	Functional	intersects with	Heuristic / Nonsignature-Based Detection	END-04.4	Mechanisms exist to utilize heuristic / nonsignature-based antimalware detection capabilities.	5	Essential Eight: ML3
ISM-1891	N/A	Microsoft Office macros digitally signed by signatures other than V3 signatures cannot be enabled via the Message Bar or Backstage View.			ML3	Functional	subset of	Signed Components	CHG-04.2	Mechanisms exist to prevent the installation of software and firmware components without verification that the component has been digitally signed using an organization-approved certificate authority.	10	Essential Eight: ML3
ISM-1892	N/A	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.	ML1	ML2	ML3	Functional	subset of	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	10	Essential Eight: ML1, ML2, ML3
ISM-1893	N/A	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.	ML1	ML2	ML3	Functional	subset of	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	10	Essential Eight: ML1, ML2, ML3
ISM-1894	N/A	Multi-factor authentication used for authenticating users of data repositories is phishing-resistant.			ML3	Functional	subset of	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	10	Essential Eight: ML3
ISM-1895	N/A	Successful and unsuccessful single-factor authentication events are centrally logged.				Functional	intersects with	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data privacy and supply chain activities to achieve integrated situational awareness.	5	
ISM-1895	N/A	Successful and unsuccessful single-factor authentication events are centrally logged.				Functional	intersects with	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	
ISM-1895	N/A	Successful and unsuccessful single-factor authentication events are centrally logged.				Functional	intersects with	Content of Event Logs	MON-03	Mechanisms exist to configure systems to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5	
ISM-1896	N/A	Memory integrity functionality is enabled.			ML3	Functional	subset of	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	10	Essential Eight: ML3
ISM-1897	N/A	Remote Credential Guard functionality is enabled.			ML3	Functional	subset of	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	10	Essential Eight: ML3
ISM-1898	N/A	Secure Admin Workstations are used in the performance of administrative activities.			ML3	Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	Essential Eight: ML3
ISM-1898	N/A	Secure Admin Workstations are used in the performance of administrative activities.			ML3	Functional	intersects with	Dedicated Administrative Machines	IAC-20.4	Mechanisms exist to restrict executing administrative tasks or tasks requiring elevated access to a dedicated machine.	5	Essential Eight: ML3
ISM-1899	N/A	Network devices that do not belong to administrative infrastructure cannot initiate connections with administrative infrastructure.				Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
ISM-1899	N/A	Network devices that do not belong to administrative infrastructure cannot initiate connections with administrative infrastructure.				Functional	intersects with	Dedicated Administrative Machines	IAC-20.4	Mechanisms exist to restrict executing administrative tasks or tasks requiring elevated access to a dedicated machine.	5	
ISM-1900	N/A	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in firmware.			ML3	Functional	subset of	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	10	Essential Eight: ML3
ISM-1901	N/A	Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.			ML3	Functional	subset of	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	10	Essential Eight: ML3
ISM-1902	N/A	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.			ML3	Functional	subset of	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	10	Essential Eight: ML3
ISM-1903	N/A	Patches, updates or other vendor mitigations for vulnerabilities in firmware are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.			ML3	Functional	subset of	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	10	Essential Eight: ML3
ISM-1904	N/A	Patches, updates or other vendor mitigations for vulnerabilities in firmware are applied within one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.			ML3	Functional	subset of	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	10	Essential Eight: ML3
ISM-1905	N/A	Online services that are no longer supported by vendors are removed.	ML1	ML2	ML3	Functional	subset of	Unsupported Systems	TDA-17	Mechanisms exist to prevent unsupported systems by: (1) Replacing systems 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 system components required to satisfy mission/business needs.	10	Essential Eight: ML1, ML2, ML3
ISM-1906	N/A	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.		ML2	ML3	Functional	subset of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	Essential Eight: ML2, ML3
ISM-1906	N/A	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.		ML2	ML3	Functional	intersects with	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	5	Essential Eight: ML2, ML3
ISM-1906	N/A	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.		ML2	ML3	Functional	intersects with	Monitoring Reporting	MON-06	Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.	5	Essential Eight: ML2, ML3
ISM-1907	N/A	Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events.			ML3	Functional	subset of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	Essential Eight: ML3
ISM-1907	N/A	Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events.			ML3	Functional	intersects with	Monitoring Reporting	MON-06	Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.	5	Essential Eight: ML3
ISM-1908	N/A	Vulnerabilities identified in applications are publicly disclosed (where appropriate to do so) by software developers in a timely manner.				Functional	intersects with	Vulnerability Disclosure Program (VDP)	THR-06	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of products and services that receives unsolicited input from the public about vulnerabilities in organizational systems, services and processes.	5	
ISM-1908	N/A	Vulnerabilities identified in applications are publicly disclosed (where appropriate to do so) by software developers in a timely manner.				Functional	intersects with	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
ISM-1909	N/A	In resolving vulnerabilities, software developers perform root cause analysis and, to the greatest extent possible, seek to remediate entire vulnerability classes.				Functional	intersects with	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity & data privacy incidents to reduce the likelihood or impact of future incidents.	5	
ISM-1909	N/A	In resolving vulnerabilities, software developers perform root cause analysis and, to the greatest extent possible, seek to remediate entire vulnerability classes.				Functional	intersects with	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
ISM-1910	N/A	Web API calls that facilitate modification of data, or access to data not authorised for release into the public domain, are centrally logged.				Functional	subset of	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	10	
ISM-1911	N/A	Web application crashes and error messages are centrally logged.				Functional	intersects with	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	
ISM-1911	N/A	Web application crashes and error messages are centrally logged.				Functional	intersects with	Error Handling	TDA-19	Mechanisms exist to handle error conditions by: (1) Identifying potentially security-relevant error conditions; (2) Generating error messages that provide information necessary for corrective actions without revealing sensitive or potentially harmful information in error logs and administrative messages that could be exploited; and (3) Revealing error messages only to authorized personnel.	5	
ISM-1912	N/A	Network documentation includes device settings for all critical servers, high-value servers, network devices and network security appliances.				Functional	subset of	Documentation Requirements	TDA-04	Mechanisms exist to obtain, protect and distribute administrator documentation for systems that describe: (1) Secure configuration, installation and operation of the system; (2) Effective use and maintenance of security features/functions; and (3) Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	Essential 8 ML1	Essential 8 ML1	Essential 8 ML1	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
ISM-1913	N/A	Approved configurations for IT equipment are developed, implemented and maintained.				Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
ISM-1913	N/A	Approved configurations for IT equipment are developed, implemented and maintained.				Functional	intersects with	Baseline Tailoring	CFG-02.9	Mechanisms exist to allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to: (1) Mission / business functions; (2) Operational environment; (3) Specific threats or vulnerabilities; or (4) Other conditions or situations that could affect mission / business success.	5	
ISM-1914	N/A	Approved configurations for operating systems are developed, implemented and maintained.				Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
ISM-1914	N/A	Approved configurations for operating systems are developed, implemented and maintained.				Functional	intersects with	Baseline Tailoring	CFG-02.9	Mechanisms exist to allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to: (1) Mission / business functions; (2) Operational environment; (3) Specific threats or vulnerabilities; or (4) Other conditions or situations that could affect mission / business success.	5	
ISM-1915	N/A	Approved configurations for user applications are developed, implemented and maintained.				Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
ISM-1915	N/A	Approved configurations for user applications are developed, implemented and maintained.				Functional	intersects with	Baseline Tailoring	CFG-02.9	Mechanisms exist to allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to: (1) Mission / business functions; (2) Operational environment; (3) Specific threats or vulnerabilities; or (4) Other conditions or situations that could affect mission / business success.	5	
ISM-1916	N/A	Approved configurations for server applications are developed, implemented and maintained.				Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
ISM-1916	N/A	Approved configurations for server applications are developed, implemented and maintained.				Functional	intersects with	Baseline Tailoring	CFG-02.9	Mechanisms exist to allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to: (1) Mission / business functions; (2) Operational environment; (3) Specific threats or vulnerabilities; or (4) Other conditions or situations that could affect mission / business success.	5	
ISM-1917	N/A	Future cryptographic requirements and dependencies are considered during the transition to post-quantum cryptographic standards.				Functional	subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
ISM-1918	N/A	The CISO regularly reports directly to their organisation's audit, risk and compliance committee (or equivalent) on cyber security matters.				Functional	intersects with	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.	5	
ISM-1918	N/A	The CISO regularly reports directly to their organisation's audit, risk and compliance committee (or equivalent) on cyber security matters.				Functional	intersects with	Cybersecurity & Data Privacy Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	5	
ISM-1919	N/A	When multi-factor authentication is used to authenticate users or customers to online services or online customer services, all other authentication protocols that do not support multi-factor authentication are disabled.				Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
ISM-1919	N/A	When multi-factor authentication is used to authenticate users or customers to online services or online customer services, all other authentication protocols that do not support multi-factor authentication are disabled.				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 systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	5	
ISM-1920	N/A	When multi-factor authentication is used to authenticate users to online services, online customer services, systems or data repositories – that process, store or communicate their organisation's sensitive data or sensitive customer data – users are prevented from self-enrolling into multi-factor authentication from untrustworthy devices.				Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
ISM-1920	N/A	When multi-factor authentication is used to authenticate users to online services, online customer services, systems or data repositories – that process, store or communicate their organisation's sensitive data or sensitive customer data – users are prevented from self-enrolling into multi-factor authentication from untrustworthy devices.				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 systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	5	
ISM-1921	N/A	The likelihood of system compromise is frequently assessed when working exploits exist for unmitigated vulnerabilities				Functional	subset of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
ISM-1921	N/A	The likelihood of system compromise is frequently assessed when working exploits exist for unmitigated vulnerabilities				Functional	intersects with	Threat Analysis	THR-10	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.	5	
ISM-1921	N/A	The likelihood of system compromise is frequently assessed when working exploits exist for unmitigated vulnerabilities				Functional	intersects with	Vulnerability Exploitation Analysis	VPM-03.1	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats exploiting known vulnerabilities.	5	
ISM-1922	N/A	The Open Worldwide Application Security Project (OWASP) Mobile Application Security Verification Standard is used in the development of mobile applications.				Functional	subset of	Secure Practices Guidelines	OPS-05	Mechanisms exist to provide guidelines and recommendations for the secure use of products and/or services to assist in the configuration, installation and use of the product and/or service.	10	
ISM-1923	N/A	The OWASP Top 10 for Large Language Model Applications are mitigated in the development of large language model applications.				Functional	subset of	Secure Practices Guidelines	OPS-05	Mechanisms exist to provide guidelines and recommendations for the secure use of products and/or services to assist in the configuration, installation and use of the product and/or service.	10	
ISM-1924	N/A	Large language model applications evaluate the sentence perplexity of user prompts to detect and mitigate adversarial suffixes designed to assist in the generation of sensitive or harmful content.				Functional	subset of	Artificial Intelligence (AI) & Autonomous Technologies Governance	AAT-01	Mechanisms exist to ensure policies, processes, procedures and practices related to the mapping, measuring and managing of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks are in place, transparent and implemented effectively.	10	
ISM-1924	N/A	Large language model applications evaluate the sentence perplexity of user prompts to detect and mitigate adversarial suffixes designed to assist in the generation of sensitive or harmful content.				Functional	intersects with	Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV)	AAT-10	Mechanisms exist to implement Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices to enable Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related security, resilience and compliance-related conformity testing throughout the lifecycle of the AAT.	5	