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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-0009	Protecting systems and their resources	System owners, in consultation with each system's authorising officer, identify any supplementary controls required based upon the unique nature of each system, its operating environment and the organisation's risk tolerances.	Functional	Intersects With	Compensating Countermeasures	RSK-18	Mechanisms exist to identify and implement one, or more, compensating controls to reduce risk and threat exposure when the primary means of implementing the security function is unavailable or compromised.	5		RSK-06.2			
ISM-0027	Protecting systems and their resources	System owners obtain an authorisation to operate for each non-classified, OFFICIAL: Sensitive, PROTECTED and SECRET system from its authorising officer.	Functional	Intersects With	Authorize Technology Assets, Applications and/or Services (TAAS)	GOV-11.4	Mechanisms exist to compel data and/or process owners to obtain authorization for the production use of each Technology Asset, Application and/or Service (TAAS) under their control.	5		GOV-15.4			
ISM-0027	Protecting systems and their resources	System owners obtain an authorisation to operate for each non-classified, OFFICIAL: Sensitive, PROTECTED and SECRET system from its authorising officer.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-02	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10		IAO-01			
ISM-0027	Protecting systems and their resources	System owners obtain an authorisation to operate for each non-classified, OFFICIAL: Sensitive, PROTECTED and SECRET system from its authorising officer.	Functional	Intersects With	Security Authorization	IAO-14	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	5		IAO-07			
ISM-0039	Cyber security strategy	A cyber security strategy is developed, implemented and maintained.	Functional	Intersects With	Strategic Plan & Objectives	PRM-02	Mechanisms exist to establish a: (1) Strategic security, compliance and resilience-specific business plan; and (2) Set of objectives to achieve that plan.	5		PRM-01.1			
ISM-0041	System security plan	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	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-09	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and (3) Provides a historical record of applied security controls, including changes.	5		IAO-03			
ISM-0042	System administration processes and procedures	System administration processes, and supporting system administration procedures, are developed, implemented and maintained.	Functional	Intersects With	System Administrative Processes	OPS-04.1	Mechanisms exist to develop, implement and govern system administration processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining Technology Assets, Applications and/or Services (TAAS).	5		AST-26			
ISM-0043	Cyber security incident response plan	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 that 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 in a separate document.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-08	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5		IRO-04			
ISM-0047	Approval of cyber security documentation	Organisational-level cyber security documentation is approved by the chief information security officer while system-specific cyber security documentation is approved by the system's authorising officer.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-02	Mechanisms exist to facilitate the design, implementation, and monitoring of security, compliance and resilience governance controls.	10		GOV-01			
ISM-0047	Approval of cyber security documentation	Organisational-level cyber security documentation is approved by the chief information security officer while system-specific cyber security documentation is approved by the system's authorising officer.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8		GOV-02			
ISM-0072	Contractual security requirements with service providers	Security requirements associated with the confidentiality, integrity and availability of data are documented in contractual arrangements with service providers and regularly reviewed to ensure they remain fit for purpose.	Functional	Intersects With	Adequate Security for Sensitive / Regulated Data In Support of Contracts	IAO-08	Mechanisms exist to protect sensitive and/or regulated data that is collected, developed, received, transmitted, used or stored in support of the performance of a contract.	5		IAO-03.2			
ISM-0072	Contractual security requirements with service providers	Security requirements associated with the confidentiality, integrity and availability of data are documented in contractual arrangements with service providers and regularly reviewed to ensure they remain fit for purpose.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-05			
ISM-0078	Control of Australian systems	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-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10		CPL-01			
ISM-0100	Assessment of gateways	Non-classified, OFFICIAL: Sensitive, PROTECTED and SECRET gateways undergo an IRAP assessment, using the latest release of the ISM available prior to the beginning of the IRAP assessment (or a subsequent release), at least every 24 months.	Functional	Intersects With	Independent Assessors	CPL-08	Mechanisms exist to utilize independent assessors to evaluate security, compliance and resilience at planned intervals or when the Technology Asset, Application and/or Service (TAAS) undergoes significant changes.	5		CPL-03.1			
ISM-0100	Assessment of gateways	Non-classified, OFFICIAL: Sensitive, PROTECTED and SECRET gateways undergo an IRAP assessment, using the latest release of the ISM available prior to the beginning of the IRAP assessment (or a subsequent release), at least every 24 months.	Functional	Intersects With	Control Validation Testing (CVT)	IAO-04	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) 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		IAO-02			
ISM-0100	Assessment of gateways	Non-classified, OFFICIAL: Sensitive, PROTECTED and SECRET gateways undergo an IRAP assessment, using the latest release of the ISM available prior to the beginning of the IRAP assessment (or a subsequent release), at least every 24 months.	Functional	Intersects With	Specialized Assessments	IAO-05	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 and OT); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; (11) Artificial Intelligence and Autonomous Technologies (AAT); and/or (12) Other Technology Assets, Applications and/or Services (TAAS) that require specialized expertise to determine conformity with security, compliance and/or resilience requirements.	5		IAO-02.2			
ISM-0100	Assessment of gateways	Non-classified, OFFICIAL: Sensitive, PROTECTED and SECRET gateways undergo an IRAP assessment, using the latest release of the ISM available prior to the beginning of the IRAP assessment (or a subsequent release), at least every 24 months.	Functional	Intersects With	Third-Party Assessment Reciprocity	IAO-07	Mechanisms exist to accept and respond to the results of external assessments that are performed by impartial, external organizations.	5		IAO-02.3			
ISM-0109	Event log monitoring	Event logs from workstations are analysed in a timely manner to detect cyber security events.	Functional	Subset Of	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	Updated 2026.3	MON-01			
ISM-0109	Event log monitoring	Event logs from workstations are analysed in a timely manner to detect cyber security events.	Functional	Intersects With	Event Log & Security-Relevant Telemetry Monitoring	MON-03	Mechanisms exist to review event logs and security-relevant telemetry on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	Updated 2026.3	MON-01.8			
ISM-0109	Event log monitoring	Event logs from workstations are analysed in a timely manner to detect cyber security events.	Functional	Intersects With	Centralized Collection of Event Logs & Security-Relevant Telemetry	MON-05	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of event logs and security-relevant telemetry.	5	Updated 2026.3	MON-02			
ISM-0120	Event log monitoring	Cyber security personnel have access to sufficient tools to facilitate the detection of cyber security events and the identification of cyber security incidents.	Functional	Subset Of	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10		MON-01			
ISM-0120	Event log monitoring	Cyber security personnel have access to sufficient tools to facilitate the detection of cyber security events and the identification of cyber security incidents.	Functional	Intersects With	Event Log & Security-Relevant Telemetry Monitoring	MON-03	Mechanisms exist to review event logs and security-relevant telemetry on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5		MON-01.8			
ISM-0120	Event log monitoring	Cyber security personnel have access to sufficient tools to facilitate the detection of cyber security events and the identification of cyber security incidents.	Functional	Intersects With	Analyze and Prioritize Monitoring Requirements	MON-03.2	Mechanisms exist to assess the organization's needs for monitoring and prioritize the monitoring of Technology Assets, Applications and/or Services (TAAS), based on TAAS criticality and the sensitivity of the data it stores, transmits and processes.	5		MON-01.16			
ISM-0123	Reporting cyber security incidents	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 Handling	IRO-06	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	Updated 2026.3	IRO-02			
ISM-0123	Reporting cyber security incidents	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-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	Updated 2026.3	IRO-10			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-0123	Reporting cyber security incidents	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	Situational Awareness For Incidents	IRO-16.1	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	5	Updated 2026.3	IRO-09			
ISM-0125	Cyber security incident register	A cyber security incident register is developed, implemented and maintained.	Functional	Intersects With	Situational Awareness For Incidents	IRO-16.1	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	5		IRO-09			
ISM-0133	Handling and containing data spills	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-20	Mechanisms exist to respond to sensitive and/or regulated data spills.	5		IRO-12			
ISM-0133	Handling and containing data spills	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-20.3	Mechanisms exist to ensure that organizational personnel impacted by sensitive and/or regulated data spills can continue to carry out assigned tasks while contaminated Technology Assets, Applications and/or Services (TAAS) are undergoing corrective actions.	5		IRO-12.3			
ISM-0133	Handling and containing data spills	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-20.4	Mechanisms exist to address security safeguards for personnel exposed to sensitive and/or regulated data that is not within their assigned access authorizations.	5		IRO-12.4			
ISM-0133	Handling and containing data spills	When a data spill occurs, data owners are advised and access to the data is restricted.	Functional	Intersects With	Data Breach	IRO-22	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		IRO-04.1			
ISM-0137	Handling and containing intrusions	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-02	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10		IRO-01			
ISM-0137	Handling and containing intrusions	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-13	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		IRO-08			
ISM-0137	Handling and containing intrusions	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-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5		IRO-10			
ISM-0137	Handling and containing intrusions	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-16.1	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	5		IRO-09			
ISM-0138	Maintaining the integrity of evidence	The integrity of evidence gathered during an investigation is maintained by investigators: • recording all their actions • maintaining a proper chain of custody • following all instructions provided by relevant law enforcement agencies.	Functional	Intersects With	Chain of Custody & Forensics	IRO-13	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		IRO-08			
ISM-0140	Reporting cyber security incidents to ASD	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	8	Updated 2026.3	IRO-10			
ISM-0140	Reporting cyber security incidents to ASD	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.	Functional	Intersects With	Serious Incident Reporting	IRO-16.3	Mechanisms exist to report any serious incident involving the organization's Technology Assets, Applications, Services and/or Data (TAASD) to relevant authorities in the locality where the incident occurred, in accordance with mandatory reporting: (1) Requirements; and (2) Timelines.	5	Updated 2026.3	IRO-10.5			
ISM-0141	Contractual security requirements with service providers	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	Intersects With	Incident Handling	IRO-06	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		IRO-02			
ISM-0142	Reporting cryptographic-related cyber security incidents	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-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		CRY-01			
ISM-0161	Securing IT equipment and media	IT equipment and media are secured when not in use.	Functional	Intersects With	Security of Assets & Media	AST-18	Mechanisms exist to maintain strict control over Technology Assets, Applications, Services and/or Data (TAASD) to preserve confidentiality and integrity.	5		AST-05			
ISM-0161	Securing IT equipment and media	IT equipment and media are secured when not in use.	Functional	Intersects With	Unattended End-User Equipment	AST-20	Mechanisms exist to implement enhanced protection measures for unattended technology assets to protect against tampering and unauthorized access.	5		AST-06			
ISM-0164	Preventing observation by unauthorised people	Unauthorised people are prevented from observing systems, in particular workstation displays and keyboards, within facilities.	Functional	Intersects With	Working in Secure Areas	PES-11	Physical security mechanisms exist to allow only authorized personnel access to secure areas.	5		PES-04.1			
ISM-0164	Preventing observation by unauthorised people	Unauthorised people are prevented from observing systems, in particular workstation displays and keyboards, within facilities.	Functional	Intersects With	Visitor Control	PES-14	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		PES-06			
ISM-0164	Preventing observation by unauthorised people	Unauthorised people are prevented from observing systems, in particular workstation displays and keyboards, within facilities.	Functional	Intersects With	Restrict Unescorted Access	PES-14.3	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		PES-06.3			
ISM-0181	Cabling infrastructure standards	Cabling infrastructure is installed in accordance with relevant Australian Standards, as directed by the Australian Communications and Media Authority.	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-0187	Common cable bundles and conduits	SECRET cables, when bundled together or run in conduit, are run exclusively in their own individual cable bundle or conduit.	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-0194	Sealing cable reticulation systems and conduits	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	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-0195	Sealing cable reticulation systems and conduits	In shared facilities, uniquely identifiable SCEC-approved tamper-evident seals are used to seal all removable covers on TOP SECRET cable reticulation systems.	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-0198	Audio secure rooms	When penetrating a TOP SECRET audio secure room, the Australian Security Intelligence Organisation is consulted and all directions provided are complied with.	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-0201	Labelling conduits	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-11	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		DCH-04			
ISM-0201	Labelling conduits	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-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-0206	Cable labelling processes and procedures	Cable labelling processes, and supporting cable labelling procedures, are developed, implemented and maintained.	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-0208	Cable register	A cable register contains the following for each cable: • cable identifier • cable colour • sensitivity/classification • source • destination • location • seal numbers (if applicable).	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-0211	Cable register	A cable register is developed, implemented, maintained and regularly verified.	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-0213	Terminating cables on patch panels	SECRET and TOP SECRET cables are terminated on their own individual patch panels.	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-0216	Physical separation of cabinets and patch panels	TOP SECRET patch panels are installed in individual TOP SECRET cabinets.	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-0217	Physical separation of cabinets and patch panels	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	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-0218	Fly lead installation	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	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-0225	Bringing radio frequency and infrared devices into facilities	Unauthorised RF and IR devices are not brought into SECRET and TOP SECRET areas.	Functional	Intersects With	Wireless Networking	NET-24	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5		NET-15			
ISM-0229	Personnel awareness	Personnel are advised of the permitted sensitivity or classification of information that can be discussed over internal and external telephone systems.	Functional	Intersects With	Social Media & Social Networking Restrictions	HRS-06.2	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.	5		HRS-05.2			
ISM-0229	Personnel awareness	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 Mobile Devices	HRS-06.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5		HRS-05.5			
ISM-0230	Personnel awareness	Personnel are advised of security risks posed by non-secure telephone systems in areas where sensitive or classified conversations can occur.	Functional	Intersects With	Social Media & Social Networking Restrictions	HRS-06.2	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.	5		HRS-05.2			
ISM-0230	Personnel awareness	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-06.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5		HRS-05.5			
ISM-0231	Personnel awareness	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	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03			
ISM-0231	Personnel awareness	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		END-14			
ISM-0232	Protecting conversations	Telephone systems used for sensitive or classified conversations encrypt all traffic that passes over external systems.	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03			
ISM-0233	Cordless telephone systems	Cordless telephone handsets and headsets are not used for sensitive or classified conversations unless all communications are encrypted using ASD-approved cryptography.	Functional	Intersects With	Bluetooth & Wireless Devices	CFG-04.9	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		AST-14.1			
ISM-0233	Cordless telephone systems	Cordless telephone handsets and headsets are not used for sensitive or classified conversations unless all communications are encrypted using ASD-approved cryptography.	Functional	Intersects With	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5		CRY-01			
ISM-0233	Cordless telephone systems	Cordless telephone handsets and headsets are not used for sensitive or classified conversations unless all communications are encrypted using ASD-approved cryptography.	Functional	Intersects With	Social Media & Social Networking Restrictions	HRS-06.2	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.	5		HRS-05.2			
ISM-0235	Speakerphones	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	Intersects With	Social Media & Social Networking Restrictions	HRS-06.2	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.	5		HRS-05.2			
ISM-0236	Off-hook audio protection	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	Intersects With	Social Media & Social Networking Restrictions	HRS-06.2	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.	5		HRS-05.2			
ISM-0240	Using paging, message services and messaging apps	Paging, Multimedia Message Service, Short Message Service and messaging apps are not used to communicate sensitive or classified data.	Functional	Intersects With	Social Media & Social Networking Restrictions	HRS-06.2	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.	5		HRS-05.2			
ISM-0240	Using paging, message services and messaging apps	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-06.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5		HRS-05.5			
ISM-0245	Connecting multifunction devices to digital telephone systems	MFDs are not connected to digital telephone systems.	Functional	Intersects With	Multi-Function Devices (MFD)	CFG-04.12	Mechanisms exist to securely configure Multi-Function Devices (MFD) according to industry-recognized secure practices for the type of device.	5		AST-23			
ISM-0246	Emanation security risk assessments	When an emanation security risk assessment is required, it is sought as early as possible in a system's life cycle.	Functional	Intersects With	Information Leakage Due To Electromagnetic Signals Emanations	PES-30	Facility security mechanisms exist to protect the system from information leakage due to electromagnetic signals emanations.	5		PES-13			
ISM-0249	Emanation security risk assessments	System owners deploying SECRET or TOP SECRET systems in mobile platforms, or as a deployable capability, contact ASD for an emanation security risk assessment.	Functional	Intersects With	Information Leakage Due To Electromagnetic Signals Emanations	PES-30	Facility security mechanisms exist to protect the system from information leakage due to electromagnetic signals emanations.	5		PES-13			
ISM-0250	Electromagnetic interference/electromagnetic compatibility standards	IT equipment meets industry and government standards relating to electromagnetic interference/electromagnetic compatibility.	Functional	Intersects With	Information Leakage Due To Electromagnetic Signals Emanations	PES-30	Facility security mechanisms exist to protect the system from information leakage due to electromagnetic signals emanations.	5		PES-13			
ISM-0252	Providing cyber security awareness training	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	Security, Compliance & Resilience-Minded Workforce	SAT-02	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10		SAT-01			
ISM-0252	Providing cyber security awareness training	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	Security, Compliance & Resilience Awareness Training	SAT-04	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5		SAT-02			
ISM-0258	Web usage policy	A web usage policy is developed, implemented and maintained.	Functional	Intersects With	Terms of Employment	HRS-06	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to enable secure, compliant and resilient capabilities.	5		HRS-05			
ISM-0258	Web usage policy	A web usage policy is developed, implemented and maintained.	Functional	Intersects With	Web Security Policy	WEB-01	Mechanisms exist to establish a formal, documented web security policy that: (1) Conveys executive management's intent; (2) Provides organizational direction and expected behaviors; (3) Is reviewed at least annually; and (4) Is updated, as necessary, to adapt to evolving risks.	5	Updated 2026.3				
ISM-0260	Using web proxies	All web access, including that by internal servers, is conducted through web proxies.	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		NET-18.1			
ISM-0261	Web proxy event logging	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	Intersects With	Proxy Logging	MON-22.1	Mechanisms exist to log all Internet-bound requests, in order to identify prohibited activities and assist incident handlers with identifying potentially compromised systems.	5		MON-01.9			
ISM-0263	Transport Layer Security filtering	TLS traffic communicated through gateways is decrypted and inspected.	Functional	Intersects With	Visibility of Encrypted Communications	NET-20	Mechanisms exist to configure the proxy to make encrypted communications traffic visible to monitoring tools and mechanisms.	5		NET-18.2			
ISM-0264	Email usage policy	An email usage policy is developed, implemented and maintained.	Functional	Intersects With	Social Media & Social Networking Restrictions	HRS-06.2	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.	5		HRS-05.2			
ISM-0264	Email usage policy	An email usage policy is developed, implemented and maintained.	Functional	Intersects With	Electronic Messaging	NET-40.1	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5		NET-13			
ISM-0267	Webmail services	Access to non-approved webmail services is blocked.	Functional	Intersects With	Social Media & Social Networking Restrictions	HRS-06.2	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.	5		HRS-05.2			
ISM-0267	Webmail services	Access to non-approved webmail services is blocked.	Functional	Intersects With	DNS & Content Filtering	NET-17	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		NET-18			
ISM-0267	Webmail services	Access to non-approved webmail services is blocked.	Functional	Intersects With	Electronic Messaging	NET-40.1	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5		NET-13			
ISM-0269	Email distribution lists	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	Intersects With	Electronic Messaging	NET-40.1	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5		NET-13			
ISM-0270	Protective markings for emails	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-04	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5		DCH-02			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-0270	Protective markings for emails	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-11	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		DCH-04			
ISM-0270	Protective markings for emails	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-40.1	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5		NET-13			
ISM-0271	Protective marking tools	Protective marking tools do not automatically insert protective markings into emails.	Functional	Intersects With	Data & Asset Classification	DCH-04	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5		DCH-02			
ISM-0271	Protective marking tools	Protective marking tools do not automatically insert protective markings into emails.	Functional	Intersects With	Automated Marking	DCH-11.1	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		DCH-04.1			
ISM-0271	Protective marking tools	Protective marking tools do not automatically insert protective markings into emails.	Functional	Intersects With	Electronic Messaging	NET-40.1	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5		NET-13			
ISM-0272	Protective marking tools	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-04	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5		DCH-02			
ISM-0272	Protective marking tools	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-11	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		DCH-04			
ISM-0272	Protective marking tools	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-40.1	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5		NET-13			
ISM-0280	Evaluated product selection	If procuring an evaluated product, a product that has completed a PP-based evaluation, including against all applicable PP modules (as well as a software bill of materials assessment if applicable), is selected in preference to one that has completed an EAL-based evaluation.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-02	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10		IAO-01			
ISM-0285	Delivery of evaluated products	Evaluated products are delivered in a manner consistent with any delivery procedures defined in associated evaluation documentation.	Functional	Subset Of	Asset Governance	AST-02	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10		AST-01			
ISM-0286	Delivery of evaluated products	When procuring high assurance information technology (IT) equipment, ASD is contacted for any equipment-specific delivery procedures.	Functional	Subset Of	Asset Governance	AST-02	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10		AST-01			
ISM-0289	Using evaluated products	Evaluated products are installed, configured, administered and operated in an evaluated configuration and in accordance with vendor guidance.	Functional	Subset Of	Asset Governance	AST-02	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10		AST-01			
ISM-0290	Using evaluated products	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-02	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10		AST-01			
ISM-0293	Classifying IT equipment	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-18	Mechanisms exist to maintain strict control over Technology Assets, Applications, Services and/or Data (TAASD) to preserve confidentiality and integrity.	5		AST-05			
ISM-0293	Classifying IT equipment	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-14	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	5		IAO-07			
ISM-0294	Labelling IT equipment	IT equipment, except for high assurance IT equipment, is labelled with protective markings reflecting its sensitivity or classification.	Functional	Intersects With	Data & Asset Classification	DCH-04	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5		DCH-02			
ISM-0294	Labelling IT equipment	IT equipment, except for high assurance IT equipment, is labelled with protective markings reflecting its sensitivity or classification.	Functional	Intersects With	Media Marking	DCH-11	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		DCH-04			
ISM-0296	Labelling high assurance IT equipment	ASD's approval is sought before applying labels to external surfaces of high assurance IT equipment.	Functional	Intersects With	Data & Asset Classification	DCH-04	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5		DCH-02			
ISM-0296	Labelling high assurance IT equipment	ASD's approval is sought before applying labels to external surfaces of high assurance IT equipment.	Functional	Intersects With	Media Marking	DCH-11	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		DCH-04			
ISM-0298	Patch management processes and procedures	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	Intersects With	Centralized Management of Flaw Remediation Processes	VPM-06.1	Mechanisms exist to centrally-manage the flaw remediation process.	5		VPM-05.1			
ISM-0300	Mitigating known vulnerabilities	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	Intersects With	Centralized Management of Flaw Remediation Processes	VPM-06.1	Mechanisms exist to centrally-manage the flaw remediation process.	5		VPM-05.1			
ISM-0304	Cessation of support	Applications other than office productivity suites, web browsers and their extensions, email clients, PDF applications, Adobe Flash Player, and security products that are no longer supported by vendors are removed.	Functional	Subset Of	Unsupported Technology Assets, Applications and/or Services (TAAS)	AST-39	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs.	10	Updated 2026.3	TDA-17			ML3
ISM-0305	On-site maintenance or repairs	Maintenance or repairs of IT equipment are carried out on site by an appropriately cleared technician.	Functional	Subset Of	Maintenance Operations	MNT-02	Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise.	10		MNT-01			
ISM-0305	On-site maintenance or repairs	Maintenance or repairs of IT equipment are carried out on site by an appropriately cleared technician.	Functional	Intersects With	Authorized Maintenance Personnel	MNT-14	Mechanisms exist to maintain a current list of authorized maintenance organizations or personnel.	5		MNT-06			
ISM-0305	On-site maintenance or repairs	Maintenance or repairs of IT equipment are carried out on site by an appropriately cleared technician.	Functional	Intersects With	Field Maintenance	MNT-17	Mechanisms exist to securely conduct field maintenance on geographically deployed assets.	5		MNT-08			
ISM-0306	On-site maintenance or repairs	If an appropriately cleared technician is not used to undertake maintenance or repairs to IT equipment, the technician is escorted by someone who: • has the authority to direct the technician • is appropriately cleared and briefed • is sufficiently familiar with the IT equipment to understand the work being undertaken • takes all responsible measures to ensure the integrity of the IT equipment • takes due care to ensure that data is not disclosed.	Functional	Intersects With	Maintenance Personnel Without Appropriate Access	MNT-14.1	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.	5		MNT-06.1			
ISM-0307	On-site maintenance or repairs	If an appropriately cleared technician is not used to undertake maintenance or repairs to IT equipment, the IT equipment and associated media are sanitised before maintenance or repairs.	Functional	Intersects With	Authorized Maintenance Personnel	MNT-14	Mechanisms exist to maintain a current list of authorized maintenance organizations or personnel.	5		MNT-06			
ISM-0310	Off-site maintenance or repairs	IT equipment maintained or repaired off site is handled at facilities approved for handling the sensitivity or classification of the IT equipment.	Functional	Intersects With	Off-Site Maintenance	MNT-18	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		MNT-09			
ISM-0311	Sanitising IT equipment	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-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	5		AST-09			
ISM-0311	Sanitising IT equipment	IT equipment containing media is sanitised by removing the media from the IT equipment or by sanitising the media in situ.	Functional	Intersects With	Digital & Non-Digital Media Disposal	DCH-17	Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.	5		DCH-08			
ISM-0311	Sanitising IT equipment	IT equipment containing media is sanitised by removing the media from the IT equipment or by sanitising the media in situ.	Functional	Intersects With	Digital Media Sanitization	DCH-18	Mechanisms exist to sanitize digital 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		DCH-09			
ISM-0312	Sanitising highly sensitive IT equipment	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-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	5		AST-09			
ISM-0312	Sanitising highly sensitive IT equipment	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	Digital & Non-Digital Media Disposal	DCH-17	Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.	5		DCH-08			
ISM-0313	IT equipment sanitisation processes and procedures	IT equipment sanitisation processes, and supporting IT equipment sanitisation procedures, are developed, implemented and maintained.	Functional	Intersects With	Digital Media Sanitization	DCH-18	Mechanisms exist to sanitize digital 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		DCH-09			
ISM-0315	Destroying high assurance IT equipment	High assurance IT equipment is destroyed prior to its disposal.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	5		AST-09			
ISM-0315	Destroying high assurance IT equipment	High assurance IT equipment is destroyed prior to its disposal.	Functional	Intersects With	Digital & Non-Digital Media Disposal	DCH-17	Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.	5		DCH-08			
ISM-0316	Disposal of IT equipment	Following sanitisation, destruction or declassification, a formal administrative decision is made to release IT equipment, or its waste, into the public domain.	Functional	Intersects With	Digital Media Sanitization Documentation	DCH-18.2	Mechanisms exist to supervise, track, document and verify digital media sanitization and disposal actions.	5		DCH-09.1			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-0317	Sanitising printers and multifunction devices	At least three pages of random text with no blank areas are printed on each colour printer cartridge or MFD print drum.	Functional	Intersects With	Digital Media Sanitization	DCH-18	Mechanisms exist to sanitize digital 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		DCH-09			
ISM-0318	Sanitising printers and multifunction devices	When unable to sanitise printer cartridges or MFD print drums, they are destroyed as per electrostatic memory devices.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	5		AST-09			
ISM-0321	Disposal of IT equipment	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	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	5		AST-09			
ISM-0323	Classifying media	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-04	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5		DCH-02			
ISM-0323	Classifying media	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-04.1	Mechanisms exist to ensure that Technology Assets, Applications and/or Services (TAAS) are classified according to the highest level of data sensitivity that is stored, transmitted and/or processed.	5		DCH-02.1			
ISM-0325	Reclassifying media	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-04.1	Mechanisms exist to ensure that Technology Assets, Applications and/or Services (TAAS) are classified according to the highest level of data sensitivity that is stored, transmitted and/or processed.	5		DCH-02.1			
ISM-0325	Reclassifying media	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-04.2	Mechanisms exist to reclassify data, including associated Technology Assets, Applications and/or Services (TAAS), commensurate with the security category and/or classification level of the information.	5		DCH-11			
ISM-0325	Reclassifying media	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-37.9	Mechanisms exist to reclassify data as required, due to changing business/technical requirements.	5		DCH-05.9			
ISM-0330	Reclassifying media	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-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	5		AST-09			
ISM-0330	Reclassifying media	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-04.2	Mechanisms exist to reclassify data, including associated Technology Assets, Applications and/or Services (TAAS), commensurate with the security category and/or classification level of the information.	5		DCH-11			
ISM-0332	Labelling media	Media, except for internally mounted fixed media within information technology equipment, is labelled with protective markings reflecting its sensitivity or classification.	Functional	Intersects With	Media Marking	DCH-11	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		DCH-04			
ISM-0336	IT equipment registers	A networked IT equipment register is developed, implemented, maintained and regularly verified.	Functional	Intersects With	Asset Inventories	AST-04	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5		AST-02			
ISM-0336	IT equipment registers	A networked IT equipment register is developed, implemented, maintained and regularly verified.	Functional	Intersects With	Sensitive Data Inventories	DCH-05	Mechanisms exist to maintain inventory logs of all sensitive media and conduct sensitive media inventories at least annually.	5		DCH-06.2			
ISM-0337	Classifying media	Media is only used with systems that are authorised to process, store or communicate its sensitivity or classification.	Functional	Subset Of	Data Protection	DCH-02	Mechanisms exist to facilitate the implementation of data protection controls.	10		DCH-01			
ISM-0341	Hardening operating system configurations	Automatic execution features for removable media are disabled.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-0341	Hardening operating system configurations	Automatic execution features for removable media are disabled.	Functional	Intersects With	Digital Media Use Restrictions	DCH-19	Mechanisms exist to restrict the use of types of digital media on systems or system components.	5		DCH-10			
ISM-0343	Device access control	If there is no business requirement for writing to removable media and devices, such functionality is disabled via the use of a device access control application or by disabling external communication interfaces.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-0343	Device access control	If there is no business requirement for writing to removable media and devices, such functionality is disabled via the use of a device access control application or by disabling external communication interfaces.	Functional	Intersects With	Limitations on Use & Distribution of Sensitive / Regulated Data	DCH-08	Mechanisms exist to restrict the use and distribution of sensitive and/or regulated data.	5		DCH-10.1			
ISM-0343	Device access control	If there is no business requirement for writing to removable media and devices, such functionality is disabled via the use of a device access control application or by disabling external communication interfaces.	Functional	Intersects With	Digital Media Use Restrictions	DCH-19	Mechanisms exist to restrict the use of types of digital media on systems or system components.	5		DCH-10			
ISM-0345	Device access control	External communication interfaces that allow DMA are disabled.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-0347	Using media for data transfers	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	Intersects With	Ad-Hoc Transfers	DCH-25	Mechanisms exist to secure ad-hoc exchanges of large digital files with internal or external parties.	5		DCH-17			
ISM-0348	Media sanitisation processes and procedures	Media sanitisation processes, and supporting media sanitisation procedures, are developed, implemented and maintained.	Functional	Intersects With	Digital Media Sanitization	DCH-18	Mechanisms exist to sanitize digital 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		DCH-09			
ISM-0350	Media that cannot be sanitised	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	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	5		AST-09			
ISM-0351	Volatile media sanitisation	Volatile media is sanitised by removing its power for at least 10 minutes.	Functional	Intersects With	Digital Media Sanitization	DCH-18	Mechanisms exist to sanitize digital 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		DCH-09			
ISM-0352	Volatile media sanitisation	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	Intersects With	Digital Media Sanitization	DCH-18	Mechanisms exist to sanitize digital 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		DCH-09			
ISM-0354	Non-volatile magnetic media sanitisation	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	Intersects With	Digital Media Sanitization	DCH-18	Mechanisms exist to sanitize digital 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		DCH-09			
ISM-0356	Treatment of non-volatile magnetic media following sanitisation	Following sanitisation, SECRET and TOP SECRET non-volatile magnetic media retains its classification.	Functional	Intersects With	Media Marking	DCH-11	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		DCH-04			
ISM-0356	Treatment of non-volatile magnetic media following sanitisation	Following sanitisation, SECRET and TOP SECRET non-volatile magnetic media retains its classification.	Functional	Intersects With	Digital Media Sanitization	DCH-18	Mechanisms exist to sanitize digital 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		DCH-09			
ISM-0357	Non-volatile erasable programmable read-only memory media sanitisation	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	Intersects With	Digital Media Sanitization	DCH-18	Mechanisms exist to sanitize digital 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		DCH-09			
ISM-0358	Treatment of non-volatile erasable and electrically erasable programmable read-only memory media following sanitisation	Following sanitisation, SECRET and TOP SECRET non-volatile EPROM and EEPROM media retains its classification.	Functional	Intersects With	Media Marking	DCH-11	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		DCH-04			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-0358	Treatment of non-volatile erasable and electrically erasable programmable read-only memory media following sanitisation	Following sanitisation, SECRET and TOP SECRET non-volatile EPROM and EEPROM media retains its classification.	Functional	Intersects With	Digital Media Sanitization	DCH-18	Mechanisms exist to sanitize digital 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		DCH-09			
ISM-0359	Non-volatile flash memory media sanitisation	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	Intersects With	Digital Media Sanitization	DCH-18	Mechanisms exist to sanitize digital 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		DCH-09			
ISM-0360	Treatment of non-volatile flash memory media following sanitisation	Following sanitisation, SECRET and TOP SECRET non-volatile flash memory media retains its classification.	Functional	Intersects With	Media Marking	DCH-11	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		DCH-04			
ISM-0360	Treatment of non-volatile flash memory media following sanitisation	Following sanitisation, SECRET and TOP SECRET non-volatile flash memory media retains its classification.	Functional	Intersects With	Digital Media Sanitization	DCH-18	Mechanisms exist to sanitize digital 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		DCH-09			
ISM-0361	Degaussing magnetic media	Magnetic media is destroyed using a degausser with a suitable magnetic field strength and magnetic orientation.	Functional	Intersects With	Digital Media Sanitization	DCH-18	Mechanisms exist to sanitize digital 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		DCH-09			
ISM-0362	Degaussing magnetic media	Product-specific directions provided by degausser manufacturers are followed.	Functional	Intersects With	Digital Media Sanitization	DCH-18	Mechanisms exist to sanitize digital 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		DCH-09			
ISM-0363	Media destruction processes and procedures	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-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	5		AST-09			
ISM-0363	Media destruction processes and procedures	Media destruction processes, and supporting media destruction procedures, are developed, implemented and maintained.	Functional	Intersects With	Digital & Non-Digital Media Disposal	DCH-17	Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.	5		DCH-08			
ISM-0363	Media destruction processes and procedures	Media destruction processes, and supporting media destruction procedures, are developed, implemented and maintained.	Functional	Intersects With	Digital Media Sanitization Documentation	DCH-18.2	Mechanisms exist to supervise, track, document and verify digital media sanitization and disposal actions.	5		DCH-09.1			
ISM-0368	Media destruction methods	Media destroyed using a hammer mill, disintegrator, grinder/sander or by cutting results in media waste particles no larger than 9 mm.	Functional	Intersects With	Digital & Non-Digital Media Disposal	DCH-17	Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.	5		DCH-08			
ISM-0370	Supervision of destruction	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-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	5		AST-09			
ISM-0370	Supervision of destruction	The destruction of media is performed under the supervision of at least one cleared person.	Functional	Intersects With	Digital Media Sanitization Documentation	DCH-18.2	Mechanisms exist to supervise, track, document and verify digital media sanitization and disposal actions.	5		DCH-09.1			
ISM-0371	Supervision of destruction	Personnel supervising the destruction of media supervise its handling to the point of destruction and ensure that the destruction is completed successfully.	Functional	Intersects With	Digital Media Sanitization Documentation	DCH-18.2	Mechanisms exist to supervise, track, document and verify digital media sanitization and disposal actions.	5		DCH-09.1			
ISM-0372	Supervision of accountable material destruction	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-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	5		AST-09			
ISM-0372	Supervision of accountable material destruction	The destruction of media storing accountable material is performed under the supervision of at least two cleared personnel.	Functional	Intersects With	Digital Media Sanitization Documentation	DCH-18.2	Mechanisms exist to supervise, track, document and verify digital media sanitization and disposal actions.	5		DCH-09.1			
ISM-0373	Supervision of accountable material destruction	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	Intersects With	Digital Media Sanitization Documentation	DCH-18.2	Mechanisms exist to supervise, track, document and verify digital media sanitization and disposal actions.	5		DCH-09.1			
ISM-0374	Media disposal processes and procedures	Media disposal processes, and supporting media disposal procedures, are developed, implemented and maintained.	Functional	Intersects With	Digital & Non-Digital Media Disposal	DCH-17	Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.	5		DCH-08			
ISM-0374	Media disposal processes and procedures	Media disposal processes, and supporting media disposal procedures, are developed, implemented and maintained.	Functional	Intersects With	Digital Media Sanitization Documentation	DCH-18.2	Mechanisms exist to supervise, track, document and verify digital media sanitization and disposal actions.	5	Updated 2026.3	DCH-09.1			
ISM-0375	Disposal of media	Following sanitisation, destruction or declassification, a formal administrative decision is made to release media, or its waste, into the public domain.	Functional	Intersects With	Digital & Non-Digital Media Disposal	DCH-17	Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.	5		DCH-08			
ISM-0378	Disposal of media	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-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	5		AST-09			
ISM-0378	Disposal of media	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	Digital & Non-Digital Media Disposal	DCH-17	Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.	5		DCH-08			
ISM-0380	Hardening operating system configurations	Unneeded user accounts, components, services and functionality of operating systems are disabled or removed.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-0382	Application management	Unprivileged users do not have the ability to uninstall or disable approved applications.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent	5	Updated 2026.3	CFG-02			
ISM-0382	Application management	Unprivileged users do not have the ability to uninstall or disable approved applications.	Functional	Intersects With	Restrict Roles Permitted To Install Software	CFG-12	Automated mechanisms exist to prevent the installation of software, unless the action is performed by a privileged user or service.	5	Updated 2026.3	CFG-05			
ISM-0383	Hardening operating system configurations	Default user accounts or credentials for operating systems, including for any pre-configured user accounts, are changed, disabled or removed during initial setup.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-0383	Hardening operating system configurations	Default user accounts or credentials for operating systems, including for any pre-configured user accounts, are changed, disabled or removed during initial setup.	Functional	Intersects With	Secure Settings By Default	TDA-03.2	Mechanisms exist to implement secure configuration settings by default to reduce the likelihood of Technology Assets, Applications and/or Services (TAAS) being deployed with weak security settings that would put the TAAS at a greater risk of compromise.	5		TDA-09.6			
ISM-0385	Functional separation between servers	Servers maintain effective functional separation from each other.	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5		CFG-03			
ISM-0393	Protecting database contents	Databases and their contents are classified based on the sensitivity or classification of data that they contain.	Functional	Intersects With	Data & Asset Classification	DCH-04	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5		DCH-02			
ISM-0393	Protecting database contents	Databases and their contents are classified based on the sensitivity or classification of data that they contain.	Functional	Intersects With	Database Administrative Processes	OPS-04.2	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	5		AST-28			
ISM-0400	Development, testing, staging and production environments	Development, testing, staging and production environments are segregated.	Functional	Intersects With	Secure Development Environments	TDA-15	Mechanisms exist to maintain a segmented development network to ensure a secure development environment.	5		TDA-07			
ISM-0400	Development, testing, staging and production environments	Development, testing, staging and production environments are segregated.	Functional	Intersects With	Separation of Development, Testing and Operational Environments	TDA-15.1	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 Technology Assets, Applications and/or Services (TAAS).	5		TDA-08			
ISM-0401	Secure software development	Secure by Design principles and practices are followed throughout the software development life cycle.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5		TDA-06			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-0402	Software security testing	Software is comprehensively tested for vulnerabilities using SAST, DAST and SCA prior to its initial release, any subsequent release, and periodically to help identify any previously unidentified vulnerabilities.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-17	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience 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 control testing and evaluation process; and (3) Document the results.	5		TDA-09			
ISM-0402	Software security testing	Software is comprehensively tested for vulnerabilities using SAST, DAST and SCA prior to its initial release, any subsequent release, and periodically to help identify any previously unidentified vulnerabilities.	Functional	Intersects With	Static Code Analysis	TDA-17.1	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ static code analysis tools to identify and remediate common flaws and document the results of the analysis.	5		TDA-09.2			
ISM-0402	Software security testing	Software is comprehensively tested for vulnerabilities using SAST, DAST and SCA prior to its initial release, any subsequent release, and periodically to help identify any previously unidentified vulnerabilities.	Functional	Intersects With	Dynamic Code Analysis	TDA-17.2	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ dynamic code analysis tools to identify and remediate common flaws and document the results of the analysis.	5		TDA-09.3			
ISM-0402	Software security testing	Software is comprehensively tested for vulnerabilities using SAST, DAST and SCA prior to its initial release, any subsequent release, and periodically to help identify any previously unidentified vulnerabilities.	Functional	Intersects With	Malformed Input Testing	TDA-17.3	Mechanisms exist to utilize testing methods to ensure Technology Assets, Applications and/or Services (TAAS) continue to operate as intended when subject to invalid or unexpected inputs on its interfaces.	5		TDA-09.4			
ISM-0402	Software security testing	Software is comprehensively tested for vulnerabilities using SAST, DAST and SCA prior to its initial release, any subsequent release, and periodically to help identify any previously unidentified vulnerabilities.	Functional	Intersects With	Application Penetration Testing	TDA-17.4	Mechanisms exist to perform application-level penetration testing of custom-made Technology Assets, Applications and/or Services (TAAS).	5		TDA-09.5			
ISM-0402	Software security testing	Software is comprehensively tested for vulnerabilities using SAST, DAST and SCA prior to its initial release, any subsequent release, and periodically to help identify any previously unidentified vulnerabilities.	Functional	Intersects With	Test Data Integrity	TDA-18.1	Mechanisms exist to ensure the integrity of test data through existing security, compliance and resilience controls.	5		TDA-10.1			
ISM-0405	Unprivileged access to systems	Requests for unprivileged access to systems and their resources are validated when first requested.	Functional	Intersects With	Management Approval For New or Changed Accounts	IAC-09	Mechanisms exist to ensure management approvals are required for new accounts or changes in permissions to existing accounts.	5		IAC-28.1			
ISM-0405	Unprivileged access to systems	Requests for unprivileged access to systems and their resources are validated when first requested.	Functional	Intersects With	Periodic Review of Individual & Service Account Privileges	IAC-12	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		IAC-17			
ISM-0405	Unprivileged access to systems	Requests for unprivileged access to systems and their resources are validated when first requested.	Functional	Intersects With	Library Privileges	TDA-16	Mechanisms exist to restrict software library privileges to those individuals with a pertinent business need for access.	5		CHG-04.5			
ISM-0407	Recording authorisation for personnel to access systems	A secure record is maintained for the life of systems and their resources that covers the following for each user: • their user identification • their signed agreement to abide by system usage policies • who authorised their access • when their access was granted • the level of access 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-03.2	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		IAC-01.1			
ISM-0407	Recording authorisation for personnel to access systems	A secure record is maintained for the life of systems and their resources that covers the following for each user: • their user identification • their signed agreement to abide by system usage policies • who authorised their access • when their access was granted • the level of access 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-09.1	Mechanisms exist to link system access to individual users or service accounts.	5		MON-03.2			
ISM-0408	Logon banner	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-28	Mechanisms exist to utilize system use notification / logon banners that display an approved system use notification message or banner before granting access to Technology Assets, Applications and/or Services (TAAS).	5		SEA-18			
ISM-0408	Logon banner	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-28.1	Mechanisms exist to configure Microsoft Windows-based systems to display an approved logon banner before granting access to the system.	5		SEA-18.1			
ISM-0408	Logon banner	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-28.2	Mechanisms exist to utilize a truncated system use notification / logon banner on systems not capable of displaying a logon banner from a centralized directory services technology (e.g., Active Directory and Entra ID).	5		SEA-18.2			
ISM-0409	Unprivileged access to systems by foreign nationals	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	Intersects With	Citizenship Requirements	HRS-05.2	Mechanisms exist to verify that individuals accessing a system processing, storing, or transmitting sensitive and/or regulated data meet applicable statutory, regulatory and/or contractual requirements for citizenship.	5		HRS-04.3			
ISM-0411	Unprivileged access to systems by foreign nationals	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	Intersects With	Citizenship Requirements	HRS-05.2	Mechanisms exist to verify that individuals accessing a system processing, storing, or transmitting sensitive and/or regulated data meet applicable statutory, regulatory and/or contractual requirements for citizenship.	5		HRS-04.3			
ISM-0414	User identification	Personnel granted access to systems and their resources are uniquely identifiable.	Functional	Intersects With	Identification & Authentication for Organizational Users	IAC-32	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5		IAC-02			
ISM-0415	User identification	The use of shared user accounts is strictly controlled, and personnel using such accounts are uniquely identifiable.	Functional	Intersects With	Group Authentication	IAC-21.1	Mechanisms exist to require individuals to be authenticated with an individual authenticator when a group authenticator is utilized.	5		IAC-02.1			
ISM-0415	User identification	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-32	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5		IAC-02			
ISM-0417	Single-factor authentication	When systems cannot support multi-factor authentication, single-factor authentication using passwords is implemented instead.	Functional	Intersects With	Password-Based Authentication	IAC-15	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5		IAC-10.1			
ISM-0418	Protecting credentials	Physical credentials are kept separate from systems they are used to authenticate to, except for when performing authentication activities.	Functional	Intersects With	Protection of Authenticators	IAC-14.2	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	5		IAC-10.5			
ISM-0420	User identification	Where systems process, store or communicate 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-05.2	Mechanisms exist to verify that individuals accessing a system processing, storing, or transmitting sensitive and/or regulated data meet applicable statutory, regulatory and/or contractual requirements for citizenship.	5		HRS-04.3			
ISM-0420	User identification	Where systems process, store or communicate AUSTEO, AGAO or REL data, personnel who are foreign nationals are identified as such, including by their specific nationality.	Functional	Intersects With	Citizenship Identification	IAC-13.3	Mechanisms exist to identify foreign nationals, including by their specific citizenship.	5		HRS-04.4			
ISM-0421	Password strength	Passwords used for single-factor authentication on non-classified, OFFICIAL: Sensitive and PROTECTED systems are a minimum of 15 characters.	Functional	Intersects With	Password-Based Authentication	IAC-15	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5		IAC-10.1			
ISM-0421	Password strength	Passwords used for single-factor authentication on non-classified, OFFICIAL: Sensitive and PROTECTED systems are a minimum of 15 characters.	Functional	Intersects With	User Responsibilities for Account Management	IAC-22	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 and certificates).	5		IAC-18			
ISM-0422	Password strength	Passwords used for single-factor authentication on TOP SECRET systems are a minimum of 20 characters.	Functional	Intersects With	Password-Based Authentication	IAC-15	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5		IAC-10.1			
ISM-0422	Password strength	Passwords used for single-factor authentication on TOP SECRET systems are a minimum of 20 characters.	Functional	Intersects With	User Responsibilities for Account Management	IAC-22	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 and certificates).	5		IAC-18			
ISM-0428	Session locking	Services are configured with a session lock that: • activates after a maximum of 15 minutes of user inactivity, a maximum of 12 hours of overall session time or when manually activated by users • blocks access to all session content • requires users to re-authenticate using all authentication factors to unlock the session • denies users the ability to disable the session locking mechanism.	Functional	Intersects With	Session Lock	CFG-04.3	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.	5		IAC-24			
ISM-0430	Suspension of access to systems	Access to systems and their resources are removed or suspended the same day personnel no longer have a legitimate requirement for access.	Functional	Intersects With	Personnel Transfer	HRS-11	Mechanisms exist to adjust logical and physical access authorizations to Technology Assets, Applications and/or Services (TAAS) and facilities upon personnel reassignment or transfer, in a timely manner.	5		HRS-08			
ISM-0430	Suspension of access to systems	Access to systems and their resources are removed or suspended the same day personnel no longer have a legitimate requirement for access.	Functional	Intersects With	Personnel Termination	HRS-12	Mechanisms exist to govern the termination of individual employment.	5		HRS-09			
ISM-0430	Suspension of access to systems	Access to systems and their resources are removed or suspended the same day personnel no longer have a legitimate requirement for access.	Functional	Intersects With	User Provisioning & De-Provisioning	IAC-04	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	5		IAC-07			
ISM-0430	Suspension of access to systems	Access to systems and their resources are removed or suspended the same day personnel no longer have a legitimate requirement for access.	Functional	Intersects With	Change of Roles & Duties	IAC-04.1	Mechanisms exist to revoke user access rights following changes in personnel roles and duties, if no longer necessary or permitted.	5		IAC-07.1			
ISM-0430	Suspension of access to systems	Access to systems and their resources are removed or suspended the same day personnel no longer have a legitimate requirement for access.	Functional	Intersects With	Termination of Employment	IAC-04.2	Mechanisms exist to revoke user access rights in a timely manner, upon termination of employment or contract.	5		IAC-07.2			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Australia - Information Security Manual (ISM) (June 2026)
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-0432	System access requirements	Access requirements for systems and their resources are documented in their system security plan.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-09	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and (3) Provides a historical record of applied security controls, including changes.	5		IAO-03			
ISM-0434	System access requirements	Personnel undergo appropriate employment screening and, where necessary, hold an appropriate security clearance before being granted access to systems and their resources.	Functional	Intersects With	Personnel Screening	HRS-05	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5		HRS-04			
ISM-0435	System access requirements	Personnel receive any necessary briefings before being granted access to systems and their resources.	Functional	Intersects With	Formal Indoctrination	HRS-08.1	Mechanisms exist to formally educate authorized users on proper data handling practices for all the relevant types of data to which they have access.	5		HRS-04.2			
ISM-0441	Temporary access to systems	When personnel are granted temporary access to systems and their resources, 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-08	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and (3) Proactively govern individual, group, system, service, application, guest and temporary accounts.	5		IAC-15			
ISM-0441	Temporary access to systems	When personnel are granted temporary access to systems and their resources, 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-30	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		IAC-21			
ISM-0443	Temporary access to systems	Temporary access is not granted to systems that process, store or communicate caveated or sensitive compartmented information.	Functional	Intersects With	Account Management	IAC-08	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and (3) Proactively govern individual, group, system, service, application, guest and temporary accounts.	5		IAC-15			
ISM-0445	Privileged access to systems	Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-10	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5		IAC-16	ML1	ML2	ML3
ISM-0445	Privileged access to systems	Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access.	Functional	Intersects With	Dedicated Privileged Account	IAC-10.3	Mechanisms exist to assign dedicated privileged user accounts to be used solely for duties requiring privileged access.	8	Updated 2026.3	IAC-16.4	ML1	ML2	ML3
ISM-0446	Privileged access to systems by foreign nationals	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-05.1	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		HRS-04.1			
ISM-0446	Privileged access to systems by foreign nationals	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-05.2	Mechanisms exist to verify that individuals accessing a system processing, storing, or transmitting sensitive and/or regulated data meet applicable statutory, regulatory and/or contractual requirements for citizenship.	5		HRS-04.3			
ISM-0446	Privileged access to systems by foreign nationals	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-10	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5		IAC-16			
ISM-0447	Privileged access to systems by foreign nationals	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-05.1	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		HRS-04.1			
ISM-0447	Privileged access to systems by foreign nationals	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-05.2	Mechanisms exist to verify that individuals accessing a system processing, storing, or transmitting sensitive and/or regulated data meet applicable statutory, regulatory and/or contractual requirements for citizenship.	5		HRS-04.3			
ISM-0447	Privileged access to systems by foreign nationals	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-10	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5		IAC-16			
ISM-0455	Data recovery	Where practical, cryptographic equipment, applications and libraries provide 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-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5		CRY-09			
ISM-0455	Data recovery	Where practical, cryptographic equipment, applications and libraries provide 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-10.3	Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users.	5		CRY-09.3			
ISM-0457	Cryptographic implementation assurance	Cryptographic equipment, applications or libraries that have completed a Common Criteria evaluation against an ASD-endorsed Protection Profile are used when encrypting media that contains OFFICIAL: Sensitive or PROTECTED data.	Functional	Subset Of	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		CRY-01			
ISM-0459	Encrypting media	Full disk encryption, or partial encryption where access controls only allow writing to encrypted partitions or volumes, is implemented when encrypting media.	Functional	Intersects With	Encrypting Data At Rest	CRY-07	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data at rest.	5		CRY-05			
ISM-0460	Cryptographic implementation assurance	HACE is used when encrypting media that contains SECRET or TOP SECRET data.	Functional	Subset Of	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		CRY-01			
ISM-0460	Cryptographic implementation assurance	HACE is used when encrypting media that contains SECRET or TOP SECRET data.	Functional	Intersects With	Encrypting Storage Media	CRY-07.1	Cryptographic mechanisms exist to protect the confidentiality and integrity of sensitive and/or regulated data residing on storage media.	5	Updated 2026.3	CRY-05.1			
ISM-0462	Handling encrypted IT equipment and media	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	Intersects With	Cryptographic Key Loss or Change	CRY-10.3	Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users.	5		CRY-09.3			
ISM-0465	Cryptographic implementation assurance	Cryptographic equipment, applications or libraries that have completed a Common Criteria evaluation against an ASD-endorsed Protection Profile are 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	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03			
ISM-0467	Cryptographic implementation assurance	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	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03			
ISM-0469	Using cryptographic protocols	An AACP or high assurance cryptographic protocol is used when encrypting data in transit.	Functional	Subset Of	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		CRY-01			
ISM-0469	Using cryptographic protocols	An AACP or high assurance cryptographic protocol is used when encrypting data in transit.	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03			
ISM-0471	Using cryptographic algorithms	Only AACAs or high assurance cryptographic algorithms are used by cryptographic equipment, applications and libraries.	Functional	Subset Of	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		CRY-01			
ISM-0472	Using Diffie-Hellman	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-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		CRY-01			
ISM-0474	Using Elliptic Curve Diffie-Hellman	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-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		CRY-01			
ISM-0475	Using the Elliptic Curve Digital Signature Algorithm	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-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		CRY-01			
ISM-0476	Using Rivest-Shamir-Adleman	When using RSA for digital signatures, and transporting encryption session keys (and similar keys), a modulus of at least 2048 bits is used, preferably 3072 bits.	Functional	Subset Of	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		CRY-01			
ISM-0477	Using Rivest-Shamir-Adleman	When using RSA for digital signatures, and for transporting encryption session keys (and similar keys), a different key pair is used for digital signatures and transporting encryption session keys.	Functional	Subset Of	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		CRY-01			
ISM-0479	Using symmetric cryptographic algorithms	Symmetric cryptographic algorithms are not used in Electronic Codebook Mode.	Functional	Subset Of	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		CRY-01			
ISM-0481	Using cryptographic protocols	Only AACPs or high assurance cryptographic protocols are used by cryptographic equipment, applications and libraries.	Functional	Subset Of	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		CRY-01			
ISM-0484	Configuring Secure Shell	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 log in 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	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03			
ISM-0485	Authentication mechanisms	Public key-based authentication is used for SSH connections.	Functional	Intersects With	Public Key Infrastructure (PKI)	CRY-09	Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service provider.	5		CRY-08			
ISM-0487	Automated remote access	When using logins without a password for SSH connections, the following are disabled: • access from IP addresses that do not require access • port forwarding • agent credential forwarding • X11 forwarding • console access.	Functional	Intersects With	Remote Access	NET-26	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5		NET-14			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-0488	Automated remote access	If using remote access without the use of a password for SSH connections, the 'forced command' option is used to specify what command is executed and parameter checking is enabled.	Functional	Intersects With	Remote Access	NET-26	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5		NET-14			
ISM-0489	SSH-agent	When SSH-agent or similar key caching applications 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	Intersects With	Remote Access	NET-26	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5		NET-14			
ISM-0490	Configuring Secure/Multipurpose Internet Mail Extension	Versions of S/MIME earlier than S/MIME version 3.0 are not used for S/MIME connections.	Functional	Intersects With	Electronic Messaging	NET-40.1	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5		NET-13			
ISM-0494	Mode of operation	Tunnel mode is used for IPsec connections; however, if using transport mode, an IP tunnel is used.	Functional	Intersects With	Electronic Messaging	NET-40.1	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5		NET-13			
ISM-0496	Protocol selection	The ESP protocol is used for authentication and encryption of IPsec connections.	Functional	Intersects With	Electronic Messaging	NET-40.1	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5		NET-13			
ISM-0498	Security association lifetimes	A security association lifetime of less than four hours (14400 seconds) is used for IPsec connections.	Functional	Intersects With	Electronic Messaging	NET-40.1	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5		NET-13			
ISM-0499	Communications security doctrine	Communications security doctrine and policy produced by ASD for the management and operation of HACE is complied with.	Functional	Subset Of	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		CRY-01			
ISM-0501	Transporting cryptographic equipment	Keyed cryptographic equipment is transported based on the sensitivity or classification of its keying material.	Functional	Subset Of	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		CRY-01			
ISM-0507	Cryptographic key management processes and procedures	Cryptographic key management processes, and supporting cryptographic key management procedures, are developed, implemented and maintained.	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5		CRY-09			
ISM-0516	Network documentation	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	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-17	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 and/or regulated data flows.	5		AST-04			
ISM-0518	Network documentation	Network documentation is developed, implemented and maintained.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-17	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 and/or regulated data flows.	5		AST-04			
ISM-0520	Network access controls	Network access controls are implemented on networks to prevent the connection of unauthorised network devices and networked IT equipment.	Functional	Intersects With	Network Access Control (NAC)	NET-16	Automated mechanisms exist to employ Network Access Control (NAC), or a similar technology, which is capable of detecting unauthorized devices and disable network access to those unauthorized devices.	5		AST-02.5			
ISM-0521	Using Internet Protocol version 6	IPv6 functionality is disabled in dual-stack network devices unless it is being used.	Functional	Subset Of	Network Security Controls (NSC)	NET-02	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10		NET-01			
ISM-0529	Using Virtual Local Area Networks	VLANs are not used to separate network traffic between networks belonging to different security domains.	Functional	Intersects With	Virtual Local Area Network (VLAN) Separation	NET-10	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.	5		NET-06.2			
ISM-0530	Using Virtual Local Area Networks	Network devices managing VLANs are administered from the most trusted security domain.	Functional	Intersects With	Virtual Local Area Network (VLAN) Separation	NET-10	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.	5		NET-06.2			
ISM-0534	Disabling unused physical ports on network devices	Unused physical ports on network devices are disabled.	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-05	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive secure baseline configurations.	5		CFG-02.5			
ISM-0535	Using Virtual Local Area Networks	Network devices managing VLANs belonging to different security domains do not share VLAN trunks.	Functional	Intersects With	Virtual Local Area Network (VLAN) Separation	NET-10	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.	5		NET-06.2			
ISM-0536	Public wireless networks	Public wireless networks provided for public use are segregated from all other organisation networks.	Functional	Intersects With	Guest Networks	NET-22	Mechanisms exist to implement and manage a secure guest network.	5		NET-02.2			
ISM-0536	Public wireless networks	Public wireless networks provided for public use are segregated from all other organisation networks.	Functional	Intersects With	Wireless Networking	NET-24	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5		NET-15			
ISM-0546	Video-aware and voice-aware firewalls and proxies	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	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		NET-03.2			
ISM-0547	Protecting video conferencing and Internet Protocol telephony traffic	Video conferencing and IP telephony calls are conducted using a secure real-time transport protocol.	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03			
ISM-0548	Protecting video conferencing and Internet Protocol telephony traffic	Video conferencing and IP telephony calls are established using a secure session initiation protocol.	Functional	Intersects With	Video Teleconference (VTC) Security	CFG-04.16	Mechanisms exist to implement secure Video Teleconference (VTC) capabilities on endpoint devices and in designated conference rooms, to prevent potential eavesdropping.	5		AST-20			
ISM-0548	Protecting video conferencing and Internet Protocol telephony traffic	Video conferencing and IP telephony calls are established using a secure session initiation protocol.	Functional	Intersects With	Pre/Post Transmission Handling	CRY-03.2	Cryptographic mechanisms exist to ensure the confidentiality and integrity of information during preparation for transmission and during reception.	5		CRY-01.3			
ISM-0549	Traffic separation	Video conferencing and IP telephony traffic is physically or logically separated from other data traffic.	Functional	Intersects With	Voice Over Internet Protocol (VoIP) Security	CFG-04.17	Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.	5		AST-21			
ISM-0551	Video conferencing unit and Internet Protocol phone authentication	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	CFG-04.16	Mechanisms exist to implement secure Video Teleconference (VTC) capabilities on endpoint devices and in designated conference rooms, to prevent potential eavesdropping.	5		AST-20			
ISM-0551	Video conferencing unit and Internet Protocol phone authentication	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	CFG-04.17	Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.	5		AST-21			
ISM-0553	Video conferencing unit and Internet Protocol phone authentication	Authentication and authorisation is used for all actions on a video conferencing network, including call setup and changing settings.	Functional	Intersects With	Video Teleconference (VTC) Security	CFG-04.16	Mechanisms exist to implement secure Video Teleconference (VTC) capabilities on endpoint devices and in designated conference rooms, to prevent potential eavesdropping.	5		AST-20			
ISM-0554	Video conferencing unit and Internet Protocol phone authentication	An encrypted and non-replayable two-way authentication scheme is used for call authentication and authorisation.	Functional	Intersects With	Video Teleconference (VTC) Security	CFG-04.16	Mechanisms exist to implement secure Video Teleconference (VTC) capabilities on endpoint devices and in designated conference rooms, to prevent potential eavesdropping.	5		AST-20			
ISM-0554	Video conferencing unit and Internet Protocol phone authentication	An encrypted and non-replayable two-way authentication scheme is used for call authentication and authorisation.	Functional	Intersects With	Pre/Post Transmission Handling	CRY-03.2	Cryptographic mechanisms exist to ensure the confidentiality and integrity of information during preparation for transmission and during reception.	5		CRY-01.3			
ISM-0555	Video conferencing unit and Internet Protocol phone authentication	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	CFG-04.16	Mechanisms exist to implement secure Video Teleconference (VTC) capabilities on endpoint devices and in designated conference rooms, to prevent potential eavesdropping.	5		AST-20			
ISM-0555	Video conferencing unit and Internet Protocol phone authentication	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	CFG-04.17	Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.	5		AST-21			
ISM-0556	Traffic separation	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	Intersects With	Voice Over Internet Protocol (VoIP) Security	CFG-04.17	Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.	5		AST-21			
ISM-0558	Internet Protocol phones in public areas	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-31	Mechanisms exist to establish usage restrictions and implementation guidance for telecommunication equipment to prevent: (1) Potential damage; (2) Unauthorized modification; and/or (3) Potential eavesdropping.	5		AST-19			
ISM-0558	Internet Protocol phones in public areas	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	CFG-04.17	Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.	5		AST-21			
ISM-0559	Microphones and webcams	Microphones (including headsets and USB handsets) and webcams are not used with non-SECRET workstations in SECRET areas.	Functional	Intersects With	Microphones & Web Cameras	CFG-04.11	Mechanisms exist to configure assets to prohibit the use of endpoint-based microphones and web cameras in secure areas or where sensitive and/or regulated information is discussed.	5		AST-22			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-0565	Handling emails with inappropriate, invalid or missing protective markings	Email servers are configured to block, log and report emails with inappropriate protective markings.	Functional	Intersects With	Electronic Messaging	NET-40.1	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5		NET-13			
ISM-0567	Open relay email servers	Email servers only relay emails destined for or originating from their domains (including subdomains).	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-0567	Open relay email servers	Email servers only relay emails destined for or originating from their domains (including subdomains).	Functional	Intersects With	Adaptive Email Protections	NET-40.4	Mechanisms exist to utilize adaptive email protections that involve employing risk-based analysis in the application and enforcement of email protections.	5		NET-20.7			
ISM-0569	Centralised email gateways	Emails are routed via centralised email gateways.	Functional	Intersects With	Electronic Messaging	NET-40.1	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5		NET-13			
ISM-0570	Email gateway maintenance activities	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		NET-18.1			
ISM-0570	Email gateway maintenance activities	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-40.1	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5		NET-13			
ISM-0571	Centralised email gateways	When users send or receive emails, an authenticated and encrypted channel is used to route emails via their organisation's centralised email gateways.	Functional	Intersects With	Electronic Messaging	NET-40.1	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5		NET-13			
ISM-0572	Email server transport encryption	Opportunistic TLS encryption is enabled on email servers that make incoming or outgoing email connections over public network infrastructure.	Functional	Intersects With	Electronic Messaging	NET-40.1	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5		NET-13			
ISM-0574	Sender Policy Framework	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-13	Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.	5		NET-10			
ISM-0574	Sender Policy Framework	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-39.2	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		NET-10.3			
ISM-0574	Sender Policy Framework	SPF is used to specify authorised email servers (or lack thereof) for an organisation's domains (including subdomains).	Functional	Intersects With	Electronic Messaging	NET-40.1	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5		NET-13			
ISM-0576	Cyber security incident management policy	A cyber security incident management policy, and associated cyber security incident response plan, is developed, implemented and maintained.	Functional	Intersects With	Incident Response Policy	IRO-01	Mechanisms exist to establish a formal, documented incident response policy that: (1) Conveys executive management's intent; (2) Provides organizational direction and expected	5	Updated 2026.3				
ISM-0576	Cyber security incident management policy	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-02	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-	10		IRO-01			
ISM-0576	Cyber security incident management policy	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-08	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5		IRO-04			
ISM-0580	Security monitoring policy	A security monitoring policy is developed, implemented and maintained.	Functional	Intersects With	Continuous Monitoring Policy	MON-01	Mechanisms exist to establish a formal, documented continuous monitoring policy that:	8	Updated 2026.3				
ISM-0580	Security monitoring policy	A security monitoring policy is developed, implemented and maintained.	Functional	Subset Of	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10		MON-01			
ISM-0580	Security monitoring policy	A security monitoring policy is developed, implemented and maintained.	Functional	Intersects With	Analyze and Prioritize Monitoring Requirements	MON-03.2	Mechanisms exist to assess the organization's needs for monitoring and prioritize the monitoring of Technology Assets, Applications and/or Services (TAAS), based on TAAS criticality and the sensitivity of the data it stores, transmits and processes.	5		MON-01.16			
ISM-0582	Operating system event logging	Security-relevant events for Microsoft Windows operating systems are centrally logged.	Functional	Intersects With	Content of Event Logs	MON-09	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5		MON-03			
ISM-0585	Event log details	For each event logged, the date and time of the event, the relevant user or process, the relevant filename, the event description, and the information technology equipment involved are captured.	Functional	Intersects With	Content of Event Logs	MON-09	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5		MON-03			
ISM-0588	Multifunction device usage policy	An MFD usage policy is developed, implemented and maintained.	Functional	Intersects With	Social Media & Social Networking Restrictions	HRS-06.2	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.	5		HRS-05.2			
ISM-0589	Scanning and copying documents on multifunction devices	MFDs are not used to scan or copy documents above the sensitivity or classification of networks they are connected to.	Functional	Intersects With	Multi-Function Devices (MFD)	CFG-04.12	Mechanisms exist to securely configure Multi-Function Devices (MFD) according to industry-recognized secure practices for the type of device.	5		AST-23			
ISM-0590	Authenticating to multifunction devices	Authentication measures for MFDs are the same strength as those used for workstations on networks they are connected to.	Functional	Intersects With	Multi-Function Devices (MFD)	CFG-04.12	Mechanisms exist to securely configure Multi-Function Devices (MFD) according to industry-recognized secure practices for the type of device.	5		AST-23			
ISM-0591	Using peripheral switches	Evaluated peripheral switches are used when sharing peripherals between systems.	Functional	Subset Of	Asset Governance	AST-02	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10		AST-01			
ISM-0597	Consultation on Cross Domain Solutions	When planning, designing, implementing or introducing additional connectivity to CDSs, ASD is consulted and any directions provided by ASD are complied with.	Functional	Intersects With	Cross Domain Solution (CDS)	NET-41	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	5		NET-02.3			
ISM-0610	User training	Users are trained on the secure use of CDSs before access is granted.	Functional	Intersects With	Cross Domain Solution (CDS)	NET-41	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	5		NET-02.3			
ISM-0611	System administrators for gateways	System administrators for gateways are assigned the minimum privileges required to perform their duties.	Functional	Intersects With	Least Privilege	IAC-30	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		IAC-21			
ISM-0611	System administrators for gateways	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		NET-03			
ISM-0612	System administrators for gateways	System administrators for gateways are formally trained on the operation and management of gateways.	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		NET-03			
ISM-0613	System administrators for gateways	System administrators for gateways that connect to Australian Eyes Only or Releasable To networks are Australian nationals.	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		NET-03			
ISM-0616	System administrators for gateways	Separation of duties is implemented in performing administrative activities for gateways.	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		NET-03			
ISM-0619	Authenticating to networks accessed via gateways	Users authenticate to other networks accessed via gateways.	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		NET-03			
ISM-0622	Authenticating to networks accessed via gateways	IT equipment authenticates to other networks accessed via gateways.	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		NET-03			
ISM-0626	Implementing Cross Domain Solutions	CDSs are implemented between SECRET or TOP SECRET networks and any other networks belonging to different security domains.	Functional	Intersects With	Cross Domain Solution (CDS)	NET-41	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	5		NET-02.3			
ISM-0628	Implementing gateways	Gateways are implemented between networks belonging to different security domains.	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		NET-03			
ISM-0629	System administration of gateways	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-02	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10		NET-01			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-0629	System administration of gateways	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		NET-03			
ISM-0631	Implementing gateways	Gateways only allow explicitly authorised data flows.	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		NET-03			
ISM-0634	Gateway event logging	Security-relevant events for gateways are centrally logged, including: • data packets and data flows permitted through gateways • data packets and data flows attempting to leave gateways • real-time alerts for attempted intrusions.	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		NET-03			
ISM-0635	Separation of data flows	CDSs implement isolated upward and downward network paths.	Functional	Intersects With	Cross Domain Solution (CDS)	NET-41	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	5		NET-02.3			
ISM-0637	Implementing gateways	Gateways implement a demilitarised zone if external parties require access to an organisation's services.	Functional	Intersects With	De-Militarized Zone (DMZ) Monitoring	MON-25	Mechanisms exist to monitor De-Militarized Zone (DMZ) network segments to separate untrusted networks from trusted networks.	5		NET-08.1			
ISM-0637	Implementing gateways	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		NET-03			
ISM-0639	Using firewalls	Evaluated firewalls are used between networks belonging to different security domains.	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		NET-03			
ISM-0643	Using diodes	Evaluated diodes are used for controlling the data flow of unidirectional gateways between an organisation's networks and public network infrastructure.	Functional	Intersects With	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.	5		NET-04			
ISM-0645	Using diodes	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	Intersects With	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.	5		NET-04			
ISM-0649	Allowing specific content types	Files imported or exported via gateways or CDSs are filtered for allowed file types.	Functional	Intersects With	DNS & Content Filtering	NET-17	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		NET-18			
ISM-0651	Performing content filtering	Files identified by content filtering checks as malicious, or that cannot be inspected, are blocked.	Functional	Intersects With	Detonation Chambers (Sandboxes)	IRO-21	Mechanisms exist to utilize a detonation chamber capability to detect and/or block potentially-malicious files and email attachments.	5		IRO-15			
ISM-0652	Performing content filtering	Files identified by content filtering checks as suspicious are quarantined until reviewed and subsequently approved or not approved for release.	Functional	Intersects With	Detonation Chambers (Sandboxes)	IRO-21	Mechanisms exist to utilize a detonation chamber capability to detect and/or block potentially-malicious files and email attachments.	5		IRO-15			
ISM-0657	Manual import of data	When manually importing data to systems, the data is scanned for malicious and active content.	Functional	Intersects With	Sensitive / Regulated Data Sharing Decisions	DCH-08.1	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	5		DCH-14			
ISM-0659	Performing content filtering	Files imported or exported via gateways or CDSs undergo content filtering checks.	Functional	Intersects With	DNS & Content Filtering	NET-17	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		NET-18			
ISM-0660	Monitoring data import and export	Data transfer logs for SECRET and TOP SECRET systems are fully verified at least monthly.	Functional	Subset Of	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10		MON-01			
ISM-0660	Monitoring data import and export	Data transfer logs for SECRET and TOP SECRET systems are fully verified at least monthly.	Functional	Intersects With	Analyze and Prioritize Monitoring Requirements	MON-03.2	Mechanisms exist to assess the organization's needs for monitoring and prioritize the monitoring of Technology Assets, Applications and/or Services (TAAS), based on TAAS criticality and the sensitivity of the data it stores, transmits and processes.	5		MON-01.16			
ISM-0661	User responsibilities	Users transferring data to and from systems are held accountable for data transfers they perform.	Functional	Intersects With	Sensitive / Regulated Data Sharing Decisions	DCH-08.1	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	5		DCH-14			
ISM-0663	Data transfer processes and procedures	Data transfer processes, and supporting data transfer procedures, are developed, implemented and maintained.	Functional	Intersects With	Sensitive / Regulated Data Sharing Decisions	DCH-08.1	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	5		DCH-14			
ISM-0664	Authorising export of data	Data exported from SECRET and TOP SECRET systems is reviewed and authorised by a trustworthy source beforehand.	Functional	Intersects With	Sensitive / Regulated Data Sharing Decisions	DCH-08.1	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	5		DCH-14			
ISM-0665	Authorising export of data	Trustworthy sources for SECRET and TOP SECRET systems are limited to people and services that have been verified and authorised as such by the chief information security officer.	Functional	Intersects With	Sensitive / Regulated Data Sharing Decisions	DCH-08.1	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	5		DCH-14			
ISM-0665	Authorising export of data	Trustworthy sources for SECRET and TOP SECRET systems are limited to people and services that have been verified and authorised as such by the chief information security officer.	Functional	Intersects With	Zero Trust Architecture (ZTA)	NET-14	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		NET-01.1			
ISM-0669	Manual export of data	When manually exporting data from SECRET and TOP SECRET systems, digital signatures are validated and keyword checks are performed within all textual data.	Functional	Intersects With	Sensitive / Regulated Data Sharing Decisions	DCH-08.1	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	5		DCH-14			
ISM-0670	Cross Domain Solution event logging	Security-relevant events for CDSs are centrally logged.	Functional	Intersects With	Cross Domain Solution (CDS)	NET-41	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	5		NET-02.3			
ISM-0675	Authorising export of data	Data authorised for export from SECRET and TOP SECRET systems is digitally signed by a trustworthy source.	Functional	Intersects With	Sensitive / Regulated Data Sharing Decisions	DCH-08.1	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	5		DCH-14			
ISM-0677	Validating file integrity	Files imported or exported via gateways or CDSs that have a digital signature or cryptographic checksum are validated.	Functional	Intersects With	Integrity of Data In Transit	CRY-06	Cryptographic mechanisms exist to detect unauthorized changes to data in transit.	5		CRY-04			
ISM-0682	Using Bluetooth functionality	Bluetooth functionality is not enabled on SECRET and TOP SECRET mobile devices.	Functional	Subset Of	Centralized Management Of Mobile Devices	MDM-02	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	10		MDM-01			
ISM-0687	Approved mobile platforms	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-02	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	10		MDM-01			
ISM-0694	Privately owned mobile devices and desktop computers	Privately owned mobile devices and desktop computers do not access SECRET and TOP SECRET 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 Technology Assets, Applications and/or Services (TAAS).	5		MDM-06			
ISM-0701	Mobile device emergency sanitisation processes and procedures	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-06.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5		HRS-05.5			
ISM-0702	Mobile device emergency sanitisation processes and procedures	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	Intersects With	Remote Purging	MDM-09	Mechanisms exist to remotely purge selected information from mobile devices.	5		MDM-05			
ISM-0705	Mobile devices and desktop computers accessing the internet	When accessing an organisation's network via a VPN connection, split tunnelling is disabled.	Functional	Intersects With	Use of Mobile Devices	HRS-06.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5		HRS-05.5			
ISM-0705	Mobile devices and desktop computers accessing the internet	When accessing an organisation's network via a VPN connection, split tunnelling is disabled.	Functional	Intersects With	Split Tunneling	NET-03.13	Mechanisms exist to prevent split tunneling for remote devices unless the split tunnel is securely provisioned using organization-defined safeguards.	5		CFG-03.4			
ISM-0714	Providing cyber security leadership and guidance	A CISO is appointed to provide cyber security leadership and guidance for their organisation (covering IT and OT).	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-05	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 Security, Compliance & Resilience Program (SCRP).	5		GOV-04			
ISM-0717	Overseeing cyber security personnel	The CISO oversees the management of cyber security personnel within their organisation.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-05	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 Security, Compliance & Resilience Program (SCRP).	5		GOV-04			
ISM-0717	Overseeing cyber security personnel	The CISO oversees the management of cyber security personnel within their organisation.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-04	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5		HRS-03			
ISM-0718	Reporting on cyber security	The CISO regularly reports directly to their organisation's board of directors or executive committee on cyber security matters.	Functional	Intersects With	Status Reporting To Governing Body	GOV-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	5		GOV-01.2			
ISM-0720	Communicating a cyber security vision and strategy	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 Security, Compliance & Resilience Responsibilities	GOV-05	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 Security, Compliance & Resilience Program (SCRP).	5		GOV-04			
ISM-0720	Communicating a cyber security vision and strategy	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-04	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5		HRS-03			
ISM-0720	Communicating a cyber security vision and strategy	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-02	Mechanisms exist to establish a: (1) Strategic security, compliance and resilience-specific business plan; and (2) Set of objectives to achieve that plan.	5		PRM-01.1			
ISM-0720	Communicating a cyber security vision and strategy	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	Security, Compliance & Resilience Protection Portfolio Management	PRM-04	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10		PRM-01			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-0720	Communicating a cyber security vision and strategy	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	Security, Compliance & Resilience Requirements Definition	PRM-09	Mechanisms exist to proactively govern Technology Assets, Applications and/or Services (TAAS) by: (1) Defining technical security, compliance and resilience requirements; and (2) Performing a criticality analysis at predefined decision points in the Secure Development Life Cycle (SDLC).	5		PRM-05			
ISM-0720	Communicating a cyber security vision and strategy	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	Security, Compliance & Resilience-Minded Workforce	SAT-02	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10		SAT-01			
ISM-0724	Overseeing the cyber security program	The CISO implements cyber security measurement metrics and key performance indicators for their organisation.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-05	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 Security, Compliance & Resilience Program (SCRP).	5		GOV-04			
ISM-0724	Overseeing the cyber security program	The CISO implements cyber security measurement metrics and key performance indicators for their organisation.	Functional	Intersects With	Measures of Performance	GOV-12	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	5		GOV-05			
ISM-0724	Overseeing the cyber security program	The CISO implements cyber security measurement metrics and key performance indicators for their organisation.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-04	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5		HRS-03			
ISM-0725	Coordinating cyber security	The CISO coordinates cyber security and business alignment through a cyber security steering committee or advisory board, comprising key cyber security and business executives, which meets formally and regularly.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-05	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 Security, Compliance & Resilience Program (SCRP).	5		GOV-04			
ISM-0725	Coordinating cyber security	The CISO coordinates cyber security and business alignment through a cyber security steering committee or advisory board, comprising key cyber security and business executives, which meets formally and regularly.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-09	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5		GOV-01.1			
ISM-0725	Coordinating cyber security	The CISO coordinates cyber security and business alignment through a cyber security steering committee or advisory board, comprising key cyber security and business executives, which meets formally and regularly.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-04	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5		HRS-03			
ISM-0726	Coordinating cyber security	The CISO coordinates security risk management activities between cyber security and business teams.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-05	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 Security, Compliance & Resilience Program (SCRP).	5		GOV-04			
ISM-0726	Coordinating cyber security	The CISO coordinates security risk management activities between cyber security and business teams.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-04	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5		HRS-03			
ISM-0726	Coordinating cyber security	The CISO coordinates security risk management activities between cyber security and business teams.	Functional	Subset Of	Risk Management Program	RSK-02	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with: (1) The organization's Enterprise Risk Management (ERM); and (2) Industry-recognized cybersecurity risk management practices.	10		RSK-01			
ISM-0731	Working with suppliers	The CISO oversees cyber supply chain risk management activities for their organisation.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-05	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 Security, Compliance & Resilience Program (SCRP).	5		GOV-04			
ISM-0731	Working with suppliers	The CISO oversees cyber supply chain risk management activities for their organisation.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-04	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5		HRS-03			
ISM-0731	Working with suppliers	The CISO oversees cyber supply chain risk management activities for their organisation.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-20	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5		RSK-09			
ISM-0731	Working with suppliers	The CISO oversees cyber supply chain risk management activities for their organisation.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-04	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5		TPM-03			
ISM-0732	Receiving and managing a dedicated cyber security budget	The CISO receives and manages a dedicated cyber security budget for their organisation.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-05	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 Security, Compliance & Resilience Program (SCRP).	5		GOV-04			
ISM-0732	Receiving and managing a dedicated cyber security budget	The CISO receives and manages a dedicated cyber security budget for their organisation.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-04	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5		HRS-03			
ISM-0732	Receiving and managing a dedicated cyber security budget	The CISO receives and manages a dedicated cyber security budget for their organisation.	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-04	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10		PRM-01			
ISM-0732	Receiving and managing a dedicated cyber security budget	The CISO receives and manages a dedicated cyber security budget for their organisation.	Functional	Intersects With	Security, Compliance & Resilience Resource Management	PRM-05	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions.	5		PRM-02			
ISM-0732	Receiving and managing a dedicated cyber security budget	The CISO receives and manages a dedicated cyber security budget for their organisation.	Functional	Intersects With	Allocation of Resources	PRM-06	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	5		PRM-03			
ISM-0733	Overseeing cyber security incident response activities	The CISO is fully aware of all cyber security incidents within their organisation.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-05	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 Security, Compliance & Resilience Program (SCRP).	5		GOV-04			
ISM-0733	Overseeing cyber security incident response activities	The CISO is fully aware of all cyber security incidents within their organisation.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-04	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5		HRS-03			
ISM-0733	Overseeing cyber security incident response activities	The CISO is fully aware of all cyber security incidents within their organisation.	Functional	Intersects With	Integrated Security Incident Response Team (ISIRT)	IRO-11	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations.	5		IRO-07			
ISM-0733	Overseeing cyber security incident response activities	The CISO is fully aware of all cyber security incidents within their organisation.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5		IRO-10			
ISM-0733	Overseeing cyber security incident response activities	The CISO is fully aware of all cyber security incidents within their organisation.	Functional	Intersects With	Situational Awareness For Incidents	IRO-16.1	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	5		IRO-09			
ISM-0733	Overseeing cyber security incident response activities	The CISO is fully aware of all cyber security incidents within their organisation.	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-16.2	Mechanisms exist to report sensitive and/or regulated data incidents in a timely manner.	5		IRO-10.2			
ISM-0734	Contributing to business continuity and disaster recovery planning	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-02	Mechanisms exist to operate a Business Continuity Management System (BCMS) to achieve resilient Technology Assets, Applications, Services and/or Data (TAASD) during: (1) Routine operations; and (2) Adverse conditions.	10		BCD-01			
ISM-0734	Contributing to business continuity and disaster recovery planning	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 Security, Compliance & Resilience Responsibilities	GOV-05	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 Security, Compliance & Resilience Program (SCRP).	5		GOV-04			
ISM-0734	Contributing to business continuity and disaster recovery planning	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-04	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5		HRS-03			
ISM-0735	Overseeing cyber security awareness training	The CISO oversees the development, implementation and maintenance of their organisation's cyber security awareness training program.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-05	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 Security, Compliance & Resilience Program (SCRP).	5		GOV-04			
ISM-0735	Overseeing cyber security awareness training	The CISO oversees the development, implementation and maintenance of their organisation's cyber security awareness training program.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-04	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5		HRS-03			
ISM-0735	Overseeing cyber security awareness training	The CISO oversees the development, implementation and maintenance of their organisation's cyber security awareness training program.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-02	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10		SAT-01			
ISM-0810	Physical access to systems	Classified systems are secured in facilities that meet the requirements for a security zone suitable for their classification.	Functional	Subset Of	Physical & Environmental Protections	PES-02	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10		PES-01			
ISM-0813	Physical access to servers, network devices and cryptographic equipment	Server rooms, communications rooms and security containers are not left in unsecured states.	Functional	Intersects With	Access To Critical Systems	PES-12	Physical access control mechanisms exist to enforce physical access to critical systems or sensitive and/or regulated data, in addition to the physical access controls for the facility.	5		PES-03.4			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-0817	Reporting suspicious contact via online services	Personnel are advised of what suspicious contact via online services is and how to report it.	Functional	Intersects With	Social Engineering & Mining	SAT-06.1	Mechanisms exist to include awareness training on recognizing and reporting potential and actual instances of social engineering and social mining.	5		SAT-02.2			
ISM-0817	Reporting suspicious contact via online services	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-06.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.	5		SAT-03.2			
ISM-0820	Posting work-related information on online services	Personnel are advised not to post work-related information on unauthorised online services, and to report cases where such information is posted.	Functional	Intersects With	Rules of Behavior	HRS-06.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5		HRS-05.1			
ISM-0821	Posting personal information on online services	Personnel are advised of security risks associated with posting personal information on online services.	Functional	Intersects With	Rules of Behavior	HRS-06.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5		HRS-05.1			
ISM-0824	Sending and receiving files via online services	Personnel are advised not to send or receive files via unauthorised online services.	Functional	Intersects With	Unsupported Internet Browsers & Email Clients	CFG-15	Mechanisms exist to allow only approved Internet browsers and email clients to run on systems.	5		CFG-04.2			
ISM-0824	Sending and receiving files via online services	Personnel are advised not to send or receive files via unauthorised online services.	Functional	Intersects With	Assigned Roles & Responsibilities Awareness	HRS-04.1	Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.	5		HRS-03.1			
ISM-0824	Sending and receiving files via online services	Personnel are advised not to send or receive files via unauthorised online services.	Functional	Intersects With	Terms of Employment	HRS-06	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to enable secure, compliant and resilient capabilities.	5		HRS-05			
ISM-0824	Sending and receiving files via online services	Personnel are advised not to send or receive files via unauthorised online services.	Functional	Intersects With	Social Media & Social Networking Restrictions	HRS-06.2	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.	5		HRS-05.2			
ISM-0824	Sending and receiving files via online services	Personnel are advised not to send or receive files via unauthorised online services.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-04	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5		SAT-02			
ISM-0824	Sending and receiving files via online services	Personnel are advised not to send or receive files via unauthorised online services.	Functional	Intersects With	Suspicious Communications & Anomalous System Behavior	SAT-06.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.	5		SAT-03.2			
ISM-0829	Bringing radio frequency and infrared devices into facilities	Security measures are used to detect and respond to unauthorised RF devices in SECRET and TOP SECRET areas.	Functional	Intersects With	Rogue Wireless Detection	NET-25	Mechanisms exist to test for the presence of Wireless Access Points (WAPs) and identify all authorized and unauthorized WAPs within the facility(ies).	5		NET-15.5			
ISM-0831	Handling media	Media is handled in a manner suitable for its sensitivity or classification.	Functional	Subset Of	Data Protection	DCH-02	Mechanisms exist to facilitate the implementation of data protection controls.	10		DCH-01			
ISM-0831	Handling media	Media is handled in a manner suitable for its sensitivity or classification.	Functional	Intersects With	Sensitive / Regulated Data Storage, Handling & Processing	SAT-05.1	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive and/or regulated data is formally trained in data handling requirements.	5		SAT-03.3			
ISM-0835	Treatment of volatile media following sanitisation	Following sanitisation, TOP SECRET volatile media retains its classification if it stored static data for an extended period, or had data repeatedly stored on or written to the same memory location for an extended period.	Functional	Intersects With	Digital Media Sanitization	DCH-18	Mechanisms exist to sanitize digital 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		DCH-09			
ISM-0836	Non-volatile electrically erasable programmable read-only memory media sanitisation	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	Intersects With	Digital Media Sanitization	DCH-18	Mechanisms exist to sanitize digital 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		DCH-09			
ISM-0839	Outsourcing media destruction	The destruction of media storing accountable material is not outsourced.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	5		AST-09			
ISM-0839	Outsourcing media destruction	The destruction of media storing accountable material is not outsourced.	Functional	Intersects With	Digital & Non-Digital Media Disposal	DCH-17	Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.	5		DCH-08			
ISM-0840	Outsourcing media destruction	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	Intersects With	Digital & Non-Digital Media Disposal	DCH-17	Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.	5		DCH-08			
ISM-0843	Application control	Application control is implemented on workstations.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-14.1	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5	Updated 2026.3	CFG-03.3			
ISM-0846	Application control	All users, except for local administrator accounts and break glass accounts, cannot disable, bypass or be exempted from application control.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5	Updated 2026.3	CFG-02			
ISM-0846	Application control	All users, except for local administrator accounts and break glass accounts, cannot disable, bypass or be exempted from application control.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-14.1	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5		CFG-03.3			
ISM-0853	Session termination	User sessions are terminated and workstations are restarted at least daily.	Functional	Intersects With	Session Termination	CFG-04.5	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.	5		IAC-25			
ISM-0854	Control of Australian systems	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-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10		CPL-01			
ISM-0861	DomainKeys Identified Mail	DKIM signing is enabled on emails originating from an organisation's domains (including subdomains).	Functional	Intersects With	Domain Name Service (DNS) Resolution	NET-13	Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.	5		NET-10			
ISM-0861	DomainKeys Identified Mail	DKIM signing is enabled on emails originating from an organisation's domains (including subdomains).	Functional	Intersects With	Electronic Messaging	NET-40.1	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5		NET-13			
ISM-0863	Maintaining mobile device security	Mobile devices prevent personnel from installing non-approved applications once provisioned.	Functional	Subset Of	Centralized Management Of Mobile Devices	MDM-02	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	10		MDM-01			
ISM-0864	Maintaining mobile device security	Mobile devices prevent personnel from disabling or modifying security functionality once provisioned.	Functional	Subset Of	Centralized Management Of Mobile Devices	MDM-02	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	10		MDM-01			
ISM-0866	Using mobile devices in public spaces	Sensitive or classified data is not viewed on mobile devices in public locations unless care is taken to reduce the chance of the screen of a mobile device being observed.	Functional	Intersects With	Use of Mobile Devices	HRS-06.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5		HRS-05.5			
ISM-0869	Encrypted storage	Mobile devices encrypt their internal storage and any removable media using ASD-approved cryptography.	Functional	Intersects With	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5		CRY-01			
ISM-0869	Encrypted storage	Mobile devices encrypt their internal storage and any removable media using ASD-approved cryptography.	Functional	Intersects With	Full Device & Container-Based Encryption	MDM-04	Cryptographic mechanisms exist to protect the confidentiality and integrity of information on mobile devices through full-device or container encryption.	5		MDM-03			
ISM-0870	Maintaining control of mobile devices	Mobile devices are carried or stored in a secured state when not being actively used.	Functional	Intersects With	Use of Mobile Devices	HRS-06.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5		HRS-05.5			
ISM-0871	Maintaining control of mobile devices	Mobile devices are kept under continual direct supervision when being actively used.	Functional	Intersects With	Use of Mobile Devices	HRS-06.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5		HRS-05.5			
ISM-0874	Mobile devices and desktop computers accessing the internet	Mobile devices and desktop computers access the internet via an organisation's internet gateway rather than via a direct connection to the internet.	Functional	Intersects With	Use of Mobile Devices	HRS-06.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5		HRS-05.5			
ISM-0874	Mobile devices and desktop computers accessing the internet	Mobile devices and desktop computers access the internet via an organisation's internet gateway rather than via a direct connection to the internet.	Functional	Subset Of	Centralized Management Of Mobile Devices	MDM-02	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	10		MDM-01			
ISM-0888	Maintenance of cyber security documentation	Cyber security documentation is reviewed at least annually and includes a 'current as at [date]' or equivalent statement.	Functional	Subset Of	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-04.1	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	10		GOV-03			
ISM-0912	Change and configuration management plan	Systems have a change and configuration management plan that includes: • the establishment and maintenance of authorised baseline configurations for systems • what constitutes routine and urgent changes to the configuration of systems • how changes to the configuration of systems will be requested, tracked and documented • who needs to be consulted prior to routine and urgent changes to the configuration of systems • who needs to approve routine and urgent changes to the configuration of systems • who needs to be notified of routine and urgent changes to the configuration of systems • what additional change management and configuration management processes and procedures need to be followed before, during and after routine and urgent changes to the configuration of systems.	Functional	Intersects With	Configuration Management Program	CFG-02	Mechanisms exist to facilitate the implementation of configuration management controls.	5		CFG-01			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-0912	Change and configuration management plan	Systems have a change and configuration management plan that includes: • the establishment and maintenance of authorised baseline configurations for systems • what constitutes routine and urgent changes to the configuration of systems • how changes to the configuration of systems will be requested, tracked and documented • who needs to be consulted prior to routine and urgent changes to the configuration of systems • who needs to approve routine and urgent changes to the configuration of systems • who needs to be notified of routine and urgent changes to the configuration of systems • what additional change management and configuration management processes and procedures need to be followed before, during and after routine and urgent changes to the configuration of systems.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-09	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and (3) Provides a historical record of applied security controls, including changes.	5		IAO-03			
ISM-0917	Handling and containing malicious code infections	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 applications are 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-06	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		IRO-02			
ISM-0917	Handling and containing malicious code infections	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 applications are 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-08	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5		IRO-04			
ISM-0926	Cable colours	Non-classified, OFFICIAL: Sensitive and PROTECTED cables are coloured neither salmon pink nor red.	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-0931	Off-hook audio protection	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	Intersects With	Social Media & Social Networking Restrictions	HRS-06.2	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.	5		HRS-05.2			
ISM-0938	User application selection	Vendors that have demonstrated a commitment to Secure by Design and Secure by Default principles and practices, including secure programming practices and either memory-safe programming languages or less preferably memory-safe programming practices, are used for user applications.	Functional	Subset Of	Technology Development & Acquisition	TDA-02	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10		TDA-01			
ISM-0947	Using media for data transfers	When transferring data manually between two systems belonging to different security domains, rewritable media is sanitised after each data transfer.	Functional	Intersects With	Digital Media Sanitization	DCH-18	Mechanisms exist to sanitize digital 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		DCH-09			
ISM-0947	Using media for data transfers	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-25	Mechanisms exist to secure ad-hoc exchanges of large digital files with internal or external parties.	5		DCH-17			
ISM-0955	Application control	Application control is implemented using cryptographic hash rules, publisher certificate rules or path rules.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-14.1	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5	Updated 2026.3	CFG-03.3			
ISM-0958	Allowing and blocking access to domain names	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	Intersects With	DNS & Content Filtering	NET-17	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		NET-18			
ISM-0961	Using web content filters	Client-side active content is restricted by web content filters to an organisation-approved list of domain names.	Functional	Intersects With	DNS & Content Filtering	NET-17	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		NET-18			
ISM-0963	Using web content filters	Web content filtering is implemented to filter potentially harmful web-based content.	Functional	Intersects With	DNS & Content Filtering	NET-17	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		NET-18			
ISM-0971	Secure web application design and development	The OWASP Application Security Verification Standard is used in the development of web applications.	Functional	Intersects With	Web Security Standard	WEB-03	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		WEB-07			
ISM-0974	Multi-factor authentication	Multi-factor authentication is used to authenticate unprivileged users of systems.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5	Updated 2026.3	IAC-06			
ISM-0974	Multi-factor authentication	Multi-factor authentication is used to authenticate unprivileged users of systems.	Functional	Intersects With	Multi-Factor Authentication (MFA) For Network Access to Non-Privileged Accounts	IAC-37.6	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for non-privileged accounts.	5	Updated 2026.3	IAC-06.2			
ISM-0988	Centralised event logging facility	An accurate and consistent time source is used for event logging.	Functional	Intersects With	System-Wide / Time-Correlated Audit Trail	MON-04.1	Automated mechanisms exist to compile audit records into an organization-wide audit trail that is time-correlated.	5		MON-02.7			
ISM-0988	Centralised event logging facility	An accurate and consistent time source is used for event logging.	Functional	Intersects With	Clock Synchronization	SEA-30	Mechanisms exist to utilize time-synchronization technology to synchronize all critical system clocks.	5		SEA-20			
ISM-0994	Asymmetric cryptographic algorithms	ECDH is used in preference to DH.	Functional	Subset Of	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		CRY-01			
ISM-0998	Integrity algorithms	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	Intersects With	Electronic Messaging	NET-40.1	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5		NET-13			
ISM-0999	Diffie-Hellman groups	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-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		CRY-01			
ISM-0999	Diffie-Hellman groups	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-40.1	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5		NET-13			
ISM-1000	Perfect Forward Secrecy	PFS is used for IPsec connections.	Functional	Intersects With	Electronic Messaging	NET-40.1	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5		NET-13			
ISM-1006	Network management traffic	Security measures are implemented to prevent unauthorised access to network management traffic.	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5		CFG-03			
ISM-1006	Network management traffic	Security measures are implemented to prevent unauthorised access to network management traffic.	Functional	Intersects With	Restrict Access To Security Functions	CFG-21	Mechanisms exist to ensure security functions are restricted to authorized individuals and enforce least privilege control requirements for necessary job functions.	5		END-16			
ISM-1013	Wireless network footprint	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	Intersects With	Wireless Boundaries	NET-24.2	Mechanisms exist to confine wireless communications to organization-controlled boundaries.	5		NET-15.4			
ISM-1014	Video conferencing unit and Internet Protocol phone authentication	Individual logins are implemented for IP phones used for SECRET or TOP SECRET conversations.	Functional	Intersects With	Video Teleconference (VTC) Security	CFG-04.16	Mechanisms exist to implement secure Video Teleconference (VTC) capabilities on endpoint devices and in designated conference rooms, to prevent potential eavesdropping.	5		AST-20			
ISM-1014	Video conferencing unit and Internet Protocol phone authentication	Individual logins are implemented for IP phones used for SECRET or TOP SECRET conversations.	Functional	Intersects With	Voice Over Internet Protocol (VoIP) Security	CFG-04.17	Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.	5		AST-21			
ISM-1019	Denial of service response plan	A denial of service response plan for video conferencing and IP telephony services is developed, implemented and maintained.	Functional	Intersects With	Denial of Service (DoS) Protection	NET-21	Automated mechanisms exist to protect against or limit the effects of denial of service attacks.	5		NET-02.1			
ISM-1023	Handling emails with inappropriate, invalid or missing protective markings	The intended recipients of blocked inbound emails, and the senders of blocked outbound emails, are notified.	Functional	Intersects With	Electronic Messaging	NET-40.1	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5		NET-13			
ISM-1024	Notifications of undeliverable emails	Notifications of undeliverable emails are only sent to senders that can be verified via SPF or other trusted means.	Functional	Intersects With	Electronic Messaging	NET-40.1	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5		NET-13			
ISM-1026	DomainKeys Identified Mail	DKIM signatures on incoming emails are verified.	Functional	Intersects With	Domain Name Service (DNS) Resolution	NET-13	Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.	5		NET-10			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-1026	DomainKeys Identified Mail	DKIM signatures on incoming emails are verified.	Functional	Intersects With	Electronic Messaging	NET-40.1	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5		NET-13			
ISM-1027	DomainKeys Identified Mail	Email distribution list applications 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-13	Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.	5		NET-10			
ISM-1027	DomainKeys Identified Mail	Email distribution list applications 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-40.1	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5		NET-13			
ISM-1028	Using Network-based Intrusion Detection and Prevention Systems	A NIDS or NIPS is deployed in gateways between an organisation's networks and other networks they do not manage.	Functional	Intersects With	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-31	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	5		NET-08			
ISM-1030	Using Network-based Intrusion Detection and Prevention Systems	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	Intersects With	Network Intrusion Detection & Prevention Systems (NIDS & NIPS)	MON-23	Mechanisms exist to monitor Network Intrusion Detection / Prevention Systems (NIDS / NIPS) technologies on critical systems, key network segments	5	Updated 2026.3	MON-01.1			
ISM-1030	Using Network-based Intrusion Detection and Prevention Systems	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	Intersects With	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-31	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	5		NET-08			
ISM-1034	Host-based intrusion detection and response solution	A HIPS or EDR solution is implemented on critical servers and high-value servers.	Functional	Intersects With	Host Intrusion Detection and Prevention Systems (HIDS / HIPS)	END-12	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		END-07			
ISM-1036	Observing multifunction device use	MFDs are placed in areas where their use can be observed.	Functional	Intersects With	Multi-Function Devices (MFD)	CFG-04.12	Mechanisms exist to securely configure Multi-Function Devices (MFD) according to industry-recognized secure practices for the type of device.	5		AST-23			
ISM-1036	Observing multifunction device use	MFDs are placed in areas where their use can be observed.	Functional	Intersects With	Access Control for Output Devices	PES-17	Physical security mechanisms exist to restrict access to printers and other system output devices to prevent unauthorized individuals from obtaining the output.	5		PES-12.2			
ISM-1037	Assessment of gateways	Gateways undergo testing following configuration changes, and at regular intervals no more than six months apart, to validate that they conform to expected security configurations.	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		NET-03			
ISM-1053	Physical access to servers, network devices and cryptographic equipment	Classified 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	Intersects With	Access To Critical Systems	PES-12	Physical access control mechanisms exist to enforce physical access to critical systems or sensitive and/or regulated data, in addition to the physical access controls for the facility.	5		PES-03.4			
ISM-1055	Insecure authentication methods	LAN Manager and NT LAN Manager authentication methods are disabled.	Functional	Intersects With	Replay-Resistant Authentication	IAC-03.1	Automated mechanisms exist to employ replay-resistant authentication.	5		IAC-02.2			
ISM-1059	Encrypting media	All data stored on media is encrypted using ASD-approved cryptography.	Functional	Intersects With	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5		CRY-01			
ISM-1059	Encrypting media	All data stored on media is encrypted using ASD-approved cryptography.	Functional	Intersects With	Encrypting Storage Media	CRY-07.1	Cryptographic mechanisms exist to protect the confidentiality and integrity of sensitive and/or regulated	8	Updated 2026.3	CRY-05.1			
ISM-1059	Encrypting media	All data stored on media is encrypted using ASD-approved cryptography.	Functional	Subset Of	Data Protection	DCH-02	Mechanisms exist to facilitate the implementation of data protection controls.	10		DCH-01			
ISM-1059	Encrypting media	All data stored on media is encrypted using ASD-approved cryptography.	Functional	Intersects With	Encrypting Data Outside of Controlled Areas	DCH-16.2	Cryptographic mechanisms exist to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	5	Updated 2026.3	DCH-07.2			
ISM-1059	Encrypting media	All data stored on media is encrypted using ASD-approved cryptography.	Functional	Intersects With	Sensitive / Regulated Data Storage, Handling & Processing	SAT-05.1	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive and/or regulated data is formally trained in data handling requirements.	5		SAT-03.3			
ISM-1065	Non-volatile magnetic media sanitisation	The host-protected area and device configuration overlay table are reset prior to the sanitisation of non-volatile magnetic hard drives.	Functional	Intersects With	Digital Media Sanitization	DCH-18	Mechanisms exist to sanitize digital 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		DCH-09			
ISM-1067	Non-volatile magnetic media sanitisation	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	Intersects With	Digital Media Sanitization	DCH-18	Mechanisms exist to sanitize digital 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		DCH-09			
ISM-1071	System ownership and oversight	Each system has a designated system owner.	Functional	Intersects With	Technology Assets, Applications, Services and/or Data (TAASD) Ownership Assignment	AST-07.1	Mechanisms exist to ensure Technology Assets, Applications, Services and/or Data (TAASD) ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organization level to establish a common understanding of requirements for asset protection.	5		AST-03			
ISM-1073	Access to systems by service providers	An organisation's systems 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-02	Mechanisms exist to facilitate the implementation of third-party management controls.	10		TPM-01			
ISM-1074	Physical access to servers, network devices and cryptographic equipment	Keys or equivalent access mechanisms to server rooms, communications rooms and security containers are appropriately controlled.	Functional	Intersects With	Access To Critical Systems	PES-12	Physical access control mechanisms exist to enforce physical access to critical systems or sensitive and/or regulated data, in addition to the physical access controls for the facility.	5		PES-03.4			
ISM-1076	Sanitising televisions and computer monitors	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.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	5		AST-09			
ISM-1078	Telephone system usage policy	A telephone system usage policy is developed, implemented and maintained.	Functional	Intersects With	Social Media & Social Networking Restrictions	HRS-06.2	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.	5		HRS-05.2			
ISM-1079	Maintenance or repairs of high assurance IT equipment	ASD's approval is sought before undertaking any maintenance or repairs to high assurance IT equipment.	Functional	Intersects With	Controlled Maintenance	MNT-03	Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application and/or Service (TAAS).	5		MNT-02			
ISM-1080	Using cryptographic algorithms	An AACA or high assurance cryptographic algorithm is used when encrypting data at rest.	Functional	Subset Of	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		CRY-01			
ISM-1080	Using cryptographic algorithms	An AACA or high assurance cryptographic algorithm is used when encrypting data at rest.	Functional	Intersects With	Encrypting Data At Rest	CRY-07	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data at rest.	5		CRY-05			
ISM-1080	Using cryptographic algorithms	An AACA or high assurance cryptographic algorithm is used when encrypting data at rest.	Functional	Intersects With	Database Encryption	CRY-08	Mechanisms exist to ensure that database servers utilize encryption to protect the confidentiality of the data within the databases.	5		CRY-05.3			
ISM-1082	Mobile device usage policy	A mobile device usage policy is developed, implemented and maintained.	Functional	Intersects With	Use of Mobile Devices	HRS-06.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5		HRS-05.5			
ISM-1082	Mobile device usage policy	A mobile device usage policy is developed, implemented and maintained.	Functional	Subset Of	Mobile Device Management Policy	MDM-01	Mechanisms exist to establish a formal, documented mobile device management policy that: (1) Conveys executive management's intent; (2) Provides organizational direction and expected behaviors; (3) Is reviewed at least annually; and (4) Is updated, as necessary, to adapt to evolving risks.	10	Updated 2026.3				
ISM-1083	Personnel awareness	Personnel are advised of the sensitivity or classification permitted for voice and data communications when using mobile devices.	Functional	Intersects With	Use of Mobile Devices	HRS-06.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5		HRS-05.5			
ISM-1084	Maintaining control of mobile devices	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	Intersects With	Use of Mobile Devices	HRS-06.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5		HRS-05.5			
ISM-1085	Encrypted communications	Mobile devices encrypt all sensitive or classified data communicated over public network infrastructure using ASD-approved cryptography.	Functional	Intersects With	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptoparaphic technologies.	5		CRY-01			
ISM-1085	Encrypted communications	Mobile devices encrypt all sensitive or classified data communicated over public network infrastructure using ASD-approved cryptography.	Functional	Subset Of	Centralized Management Of Mobile Devices	MDM-02	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	10		MDM-01			
ISM-1088	While travelling overseas with mobile devices	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-32	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		AST-24			
ISM-1088	While travelling overseas with mobile devices	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-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5		IRO-10			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-1089	Protective marking tools	Protective marking tools do not allow users replying to or forwarding emails to select protective markings lower than previously used.	Functional	Intersects With	Electronic Messaging	NET-40.1	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5		NET-13			
ISM-1091	Reporting cryptographic-related cyber security incidents	Keying material is changed when compromised or suspected of being compromised.	Functional	Subset Of	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		CRY-01			
ISM-1091	Reporting cryptographic-related cyber security incidents	Keying material is changed when compromised or suspected of being compromised.	Functional	Intersects With	Monitoring for Indicators of Compromise (IOC)	MON-17	Automated mechanisms exist to identify and alert on Indicators of Compromise (IoC).	5		MON-11.3			
ISM-1095	Labelling wall outlet boxes	Wall outlet boxes denote the systems, cable identifiers and wall outlet box identifier.	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-1096	Labelling cables	Cables are labelled at each end with sufficient source and destination details to enable the physical identification and inspection of the cable.	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-1098	Terminating cables in cabinets	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	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-1100	Terminating cables in cabinets	TOP SECRET cables are terminated in an individual TOP SECRET cabinet.	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-1101	Connecting cable reticulation systems to cabinets	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	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-1102	Connecting cable reticulation systems to cabinets	Cable reticulation systems leading into cabinets are terminated as close as possible to the cabinet.	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-1103	Connecting cable reticulation systems to cabinets	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	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-1105	Wall outlet boxes	SECRET and TOP SECRET wall outlet boxes contain exclusively SECRET or TOP SECRET cables.	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-1107	Wall outlet box colours	Non-classified, OFFICIAL: Sensitive and PROTECTED wall outlet boxes are coloured neither salmon pink nor red.	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-1107	Wall outlet box colours	Non-classified, OFFICIAL: Sensitive and PROTECTED wall outlet boxes are coloured neither salmon pink nor red.	Functional	Intersects With	Component Marking	PES-18	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		PES-16			
ISM-1109	Wall outlet box covers	Wall outlet box covers are clear plastic.	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-1111	Use of fibre-optic cables	Fibre-optic cables are used for cabling infrastructure instead of copper cables.	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-1112	Cable inspectability	Cables in non-TOP SECRET areas are inspectable every five metres or less.	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-1114	Common cable reticulation systems	Cable bundles or conduits sharing a common cable reticulation system have a dividing partition or visible gap between each cable bundle and conduit.	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-1115	Cables in walls	Cables from cable trays to wall outlet boxes are run in flexible or plastic conduit.	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-1116	Physical separation of cabinets and patch panels	A visible gap exists between TOP SECRET cabinets and non-TOP SECRET cabinets.	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-1119	Cable inspectability	Cables in TOP SECRET areas are fully inspectable for their entire length.	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-1122	Wall penetrations	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	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-1123	Power reticulation	A power distribution board with a feed from an Uninterruptible Power Supply is used to power all TOP SECRET IT equipment.	Functional	Intersects With	Emergency Power	PES-22	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.	5		PES-07.3			
ISM-1130	Enclosed cable reticulation systems	In shared facilities, cables are run in an enclosed cable reticulation system.	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-1133	Cables in party walls	In shared facilities, TOP SECRET cables are not run in party walls.	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-1137	Emanation security risk assessments	System owners deploying SECRET or TOP SECRET systems within fixed facilities contact ASD for an emanation security risk assessment.	Functional	Intersects With	Specialized Assessments	IAO-05	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 and OT); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; (11) Artificial Intelligence and Autonomous Technologies (AAT); and/or (12) Other Technology Assets, Applications and/or Services (TAAS) that require specialized expertise to determine conformity with security, compliance and/or resilience requirements.	5		IAO-02.2			
ISM-1139	Configuring Transport Layer Security	Only the latest version of TLS is used for TLS connections.	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03			
ISM-1143	Patch management processes and procedures	Patch management processes, and supporting patch management procedures, are developed, implemented and maintained.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-02	Mechanisms exist to facilitate the implementation and monitoring of risk-based vulnerability management capabilities.	10		VPM-01			
ISM-1143	Patch management processes and procedures	Patch management processes, and supporting patch management procedures, are developed, implemented and maintained.	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		VPM-05			
ISM-1145	Using mobile devices in public spaces	Privacy filters are applied to the screens of SECRET and TOP SECRET mobile devices.	Functional	Intersects With	Use of Mobile Devices	HRS-06.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5		HRS-05.5			
ISM-1146	Posting personal information on online services	Personnel are advised to maintain separate personal user accounts from any work user accounts they use for online services.	Functional	Intersects With	Terms of Employment	HRS-06	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to enable secure, compliant and resilient capabilities.	5		HRS-05			
ISM-1146	Posting personal information on online services	Personnel are advised to maintain separate personal user accounts from any work user accounts they use for online services.	Functional	Intersects With	Rules of Behavior	HRS-06.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5		HRS-05.1			
ISM-1146	Posting personal information on online services	Personnel are advised to maintain separate personal user accounts from any work user accounts they use for online services.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-04	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5		SAT-02			
ISM-1146	Posting personal information on online services	Personnel are advised to maintain separate personal user accounts from any work user accounts they use for online services.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-05	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5		SAT-03			
ISM-1151	Sender Policy Framework	SPF is used to verify the authenticity of incoming emails.	Functional	Intersects With	Domain Name Service (DNS) Resolution	NET-13	Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.	5		NET-10			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-1151	Sender Policy Framework	SPF is used to verify the authenticity of incoming emails.	Functional	Intersects With	Sender Policy Framework (SPF)	NET-39.2	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		NET-10.3			
ISM-1151	Sender Policy Framework	SPF is used to verify the authenticity of incoming emails.	Functional	Intersects With	Electronic Messaging	NET-40.1	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5		NET-13			
ISM-1157	Using diodes	Evaluated diodes are used for controlling the data flow of unidirectional gateways between networks.	Functional	Intersects With	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.	5		NET-04			
ISM-1158	Using diodes	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	Intersects With	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.	5		NET-04			
ISM-1160	Media destruction equipment	If using degaussers to destroy media, degaussers evaluated by the United States' National Security Agency are used.	Functional	Intersects With	Digital & Non-Digital Media Disposal	DCH-17	Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.	5		DCH-08			
ISM-1163	Continuous monitoring plan	Systems have a continuous monitoring plan that includes: • conducting security assessment activities to identify vulnerabilities • analysing identified vulnerabilities to determine their potential impact • implementing mitigations based on risk, effectiveness and cost.	Functional	Subset Of	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10		MON-01			
ISM-1163	Continuous monitoring plan	Systems have a continuous monitoring plan that includes: • conducting security assessment activities to identify vulnerabilities • analysing identified vulnerabilities to determine their potential impact • implementing mitigations based on risk, effectiveness and cost.	Functional	Intersects With	Analyze and Prioritize Monitoring Requirements	MON-03.2	Mechanisms exist to assess the organization's needs for monitoring and prioritize the monitoring of Technology Assets, Applications and/or Services (TAAS), based on TAAS criticality and the sensitivity of the data it stores, transmits and processes.	5		MON-01.16			
ISM-1163	Continuous monitoring plan	Systems have a continuous monitoring plan that includes: • conducting security assessment activities to identify vulnerabilities • 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-02	Mechanisms exist to facilitate the implementation and monitoring of risk-based vulnerability management capabilities.	10		VPM-01			
ISM-1163	Continuous monitoring plan	Systems have a continuous monitoring plan that includes: • conducting security assessment activities to identify vulnerabilities • analysing identified vulnerabilities to determine their potential impact • implementing mitigations based on risk, effectiveness and cost.	Functional	Intersects With	Vulnerability Ranking	VPM-05	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	5		VPM-03			
ISM-1163	Continuous monitoring plan	Systems have a continuous monitoring plan that includes: • conducting security assessment activities to identify vulnerabilities • analysing identified vulnerabilities to determine their potential impact • implementing mitigations based on risk, effectiveness and cost.	Functional	Intersects With	Vulnerability Remediation Process	VPM-06	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5		VPM-02			
ISM-1164	Covers for enclosed cable reticulation systems	In shared facilities, conduits or the front covers of ducts, cable trays in floors and ceilings, and associated fittings are clear plastic.	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-1171	Allowing and blocking access to domain names	Attempts to access websites through their IP addresses instead of their domain names are blocked by web content filters.	Functional	Intersects With	DNS & Content Filtering	NET-17	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		NET-18			
ISM-1173	Multi-factor authentication	Multi-factor authentication is used to authenticate privileged users of systems.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5	Updated 2026.3	IAC-06			
ISM-1173	Multi-factor authentication	Multi-factor authentication is used to authenticate privileged users of systems.	Functional	Intersects With	Multi-Factor Authentication (MFA) For Network Access to Privileged Accounts	IAC-37.5	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.	5	Updated 2026.3	IAC-06.1			
ISM-1175	Privileged access to systems	Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services.	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5	Updated 2026.3	CFG-03			
ISM-1175	Privileged access to systems	Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-10	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5	Updated 2026.3	IAC-16			
ISM-1175	Privileged access to systems	Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services.	Functional	Intersects With	Non-Privileged Access for Non-Security Functions	IAC-30.3	Mechanisms exist to prohibit privileged users from using privileged accounts, while performing non-security functions.	8	Updated 2026.3	IAC-21.2			
ISM-1178	Network documentation	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	Intersects With	Security of Assets & Media	AST-18	Mechanisms exist to maintain strict control over Technology Assets, Applications, Services and/or Data (TAASD) to preserve confidentiality and integrity.	5		AST-05			
ISM-1181	Network segmentation and segregation	Networks are segregated into multiple network zones according to the criticality of servers, services and data.	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network resources.	5		NET-06			
ISM-1182	Network access controls	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	Intersects With	Network Access Control (NAC)	NET-16	Automated mechanisms exist to employ Network Access Control (NAC), or a similar technology, which is capable of detecting unauthorized devices and disable network access to those unauthorized devices.	5		AST-02.5			
ISM-1183	Sender Policy Framework	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-13	Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.	5		NET-10			
ISM-1183	Sender Policy Framework	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-39.2	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		NET-10.3			
ISM-1183	Sender Policy Framework	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-40.1	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5		NET-13			
ISM-1186	Using Internet Protocol version 6	IPv6 capable network security appliances are used on IPv6 and dual-stack networks.	Functional	Subset Of	Network Security Controls (NSC)	NET-02	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10		NET-01			
ISM-1187	Manual export of data	When manually exporting data from systems, the data is checked for unsuitable protective markings.	Functional	Intersects With	Sensitive / Regulated Data Sharing Decisions	DCH-08.1	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	5		DCH-14			
ISM-1192	Implementing gateways	Gateways inspect and filter data flows at the transport and above network layers.	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		NET-03			
ISM-1195	Mobile device management policy	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-02	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	10		MDM-01			
ISM-1196	Using Bluetooth functionality	Non-classified, OFFICIAL: Sensitive and PROTECTED mobile devices are configured to remain undiscoverable to other Bluetooth devices except during Bluetooth pairing.	Functional	Intersects With	Social Media & Social Networking Restrictions	HRS-06.2	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.	5		HRS-05.2			
ISM-1196	Using Bluetooth functionality	Non-classified, 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-06.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5		HRS-05.5			
ISM-1198	Using Bluetooth functionality	Bluetooth pairing for non-classified, OFFICIAL: Sensitive and PROTECTED mobile devices is performed in a manner such that connections are only made between intended Bluetooth devices.	Functional	Intersects With	Social Media & Social Networking Restrictions	HRS-06.2	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.	5		HRS-05.2			
ISM-1198	Using Bluetooth functionality	Bluetooth pairing for non-classified, 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-06.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5		HRS-05.5			
ISM-1199	Using Bluetooth functionality	Bluetooth pairings for non-classified, OFFICIAL: Sensitive and PROTECTED mobile devices are removed when there is no longer a requirement for their use.	Functional	Intersects With	Bluetooth & Wireless Devices	CFG-04.9	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		AST-14.1			
ISM-1199	Using Bluetooth functionality	Bluetooth pairings for non-classified, OFFICIAL: Sensitive and PROTECTED mobile devices are removed when there is no longer a requirement for their use.	Functional	Intersects With	Social Media & Social Networking Restrictions	HRS-06.2	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.	5		HRS-05.2			
ISM-1199	Using Bluetooth functionality	Bluetooth pairings for non-classified, 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-06.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5		HRS-05.5			
ISM-1200	Using Bluetooth functionality	Bluetooth pairing for non-classified, OFFICIAL: Sensitive and PROTECTED mobile devices is performed using Secure Connections, preferably with Numeric Comparison if supported.	Functional	Intersects With	Bluetooth & Wireless Devices	CFG-04.9	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		AST-14.1			
ISM-1200	Using Bluetooth functionality	Bluetooth pairing for non-classified, OFFICIAL: Sensitive and PROTECTED mobile devices is performed using Secure Connections, preferably with Numeric Comparison if supported.	Functional	Intersects With	Social Media & Social Networking Restrictions	HRS-06.2	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.	5		HRS-05.2			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-1200	Using Bluetooth functionality	Bluetooth pairing for non-classified, 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-06.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5		HRS-05.5			
ISM-1203	Protecting systems and their resources	System owners, in consultation with each system's authorising officer, conduct a threat and risk assessment for each system.	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		RSK-04			
ISM-1203	Protecting systems and their resources	System owners, in consultation with each system's authorising officer, conduct a threat and risk assessment for each system.	Functional	Intersects With	Threat Analysis	THR-08	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.	5		THR-10			
ISM-1211	System administration processes and procedures	System administrators perform system administration activities in accordance with the system's change and configuration management plan.	Functional	Subset Of	Change Management Program	CHG-02	Mechanisms exist to facilitate the implementation of a change management program.	10		CHG-01			
ISM-1211	System administration processes and procedures	System administrators perform system administration activities in accordance with the system's change and configuration management plan.	Functional	Intersects With	Configuration Change Control	CHG-03	Mechanisms exist to govern the technical configuration change control processes.	5		CHG-02			
ISM-1213	Handling and containing intrusions	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-14	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	5		IRO-13			
ISM-1213	Handling and containing intrusions	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 & Security-Relevant Telemetry Retention	MON-13	Mechanisms exist to retain event logs and security-relevant telemetry 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		MON-10			
ISM-1216	Cable colour non-conformance	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-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-1216	Cable colour non-conformance	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-18	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		PES-16			
ISM-1217	Disposal of IT equipment	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-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	5		AST-09			
ISM-1217	Disposal of IT equipment	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	Digital & Non-Digital Media Disposal	DCH-17	Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.	5		DCH-08			
ISM-1217	Disposal of IT equipment	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-18	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		PES-16			
ISM-1218	Sanitising highly sensitive IT equipment	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-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	5		AST-09			
ISM-1218	Sanitising highly sensitive IT equipment	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	Digital & Non-Digital Media Disposal	DCH-17	Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.	5		DCH-08			
ISM-1219	Sanitising printers and multifunction devices	MFD print drums and image transfer rollers are inspected and destroyed if there is remnant toner that cannot be removed or a print is visible on the image transfer roller.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	5		AST-09			
ISM-1220	Sanitising printers and multifunction devices	Printer and MFD platens are inspected and destroyed if any text or images are retained on the platen.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	5		AST-09			
ISM-1221	Sanitising printers and multifunction devices	Printers and MFDs are checked to ensure no pages are trapped in the paper path due to a paper jam.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	5		AST-09			
ISM-1222	Sanitising televisions and computer monitors	Televisions and computer monitors that cannot be sanitised are destroyed.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	5		AST-09			
ISM-1223	Sanitising network devices	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	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	5		AST-09			
ISM-1227	Setting credentials for user accounts	Credentials set for user accounts are randomly generated.	Functional	Intersects With	Authenticator Management	IAC-14	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.	5		IAC-10			
ISM-1228	Event log monitoring	Cyber security events are analysed in a timely manner to identify cyber security incidents.	Functional	Intersects With	Centralized Collection of Event Logs & Security-Relevant Telemetry	MON-05	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of event logs and security-relevant telemetry.	5		MON-02		ML2	ML3
ISM-1228	Event log monitoring	Cyber security events are analysed in a timely manner to identify cyber security incidents.	Functional	Intersects With	Centralized Event Log & Security-Relevant Telemetry Review & Analysis	MON-05.1	Automated mechanisms exist to centrally collect, review and analyze event logs and security-relevant telemetry from multiple sources.	5		MON-02.2		ML2	ML3
ISM-1228	Event log monitoring	Cyber security events are analysed in a timely manner to identify cyber security incidents.	Functional	Intersects With	Correlate Monitoring Information	MON-08	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		MON-02.1		ML2	ML3
ISM-1233	Key exchange	IKE version 2 is used for key exchange when establishing IPsec connections.	Functional	Intersects With	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5		CRY-01			
ISM-1234	Email content filtering	Email content filtering is implemented to filter potentially harmful content in email bodies and attachments.	Functional	Intersects With	DNS & Content Filtering	NET-17	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		NET-18			
ISM-1235	Hardening user application configurations	Extensions for user applications are restricted to an organisation-approved set.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-14.1	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5		CFG-03.3			
ISM-1236	Allowing and blocking access to domain names	Malicious domain names, dynamic domain names and domain names that can be registered anonymously for free are blocked by web content filters.	Functional	Intersects With	DNS & Content Filtering	NET-17	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		NET-18			
ISM-1237	Using web content filters	Web content filtering is applied to outbound web traffic where appropriate.	Functional	Intersects With	DNS & Content Filtering	NET-17	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		NET-18			
ISM-1237	Using web content filters	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		NET-18.1			
ISM-1238	Secure software development	Threat modelling is used in support of the software development life cycle.	Functional	Intersects With	Threat Modeling	TDA-05.2	Mechanisms exist to perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.	5		TDA-06.2			
ISM-1239	Secure web application design and development	Robust web application frameworks are used in the development of web applications.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-05	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5		TDA-06			
ISM-1239	Secure web application design and development	Robust web application frameworks are used in the development of web applications.	Functional	Intersects With	Web Security Standard	WEB-03	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		WEB-07			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Australia - Information Security Manual (ISM) (June 2026)
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-1239	Secure web application design and development	Robust web application frameworks are used in the development of web applications.	Functional	Intersects With	Web Application Framework	WEB-04	Mechanisms exist to use a robust Web Application Framework to support the development of secure web applications, including web services, web resources and web Application Programming Interfaces (APIs).	5		WEB-08			
ISM-1240	Software input handling	Validation and sanitisation are performed on all input received over the internet by software.	Functional	Intersects With	Web Application Input Validation & Sanitization	WEB-08	Mechanisms exist to ensure all input handled by a web application is validated and/or sanitized.	5		WEB-09			
ISM-1241	Web application output encoding	Output encoding is performed on all output produced by web applications.	Functional	Intersects With	Web Application Output Encoding	WEB-10	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.	5		WEB-11			
ISM-1243	Database register	A database register is developed, implemented, maintained and regularly verified.	Functional	Intersects With	Database Administrative Processes	OPS-04.2	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	5		AST-28			
ISM-1245	Hardening server application configurations	All temporary installation files created during server application installation processes are removed after server applications have been installed.	Functional	Intersects With	Database Management System (DBMS)	AST-35	Mechanisms exist to implement and maintain Database Management Systems (DBMSs), where applicable.	5		AST-28.1			
ISM-1246	Hardening server application configurations	Server applications are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.	Functional	Intersects With	Database Management System (DBMS)	AST-35	Mechanisms exist to implement and maintain Database Management Systems (DBMSs), where applicable.	5		AST-28.1			
ISM-1247	Hardening server application configurations	Unneeded user accounts, components, services and functionality of server applications are disabled or removed.	Functional	Intersects With	Database Management System (DBMS)	AST-35	Mechanisms exist to implement and maintain Database Management Systems (DBMSs), where applicable.	5		AST-28.1			
ISM-1249	Restricting privileges for server applications	Server applications are configured to run as a separate user account with the minimum privileges needed to perform their functions.	Functional	Intersects With	Database Management System (DBMS)	AST-35	Mechanisms exist to implement and maintain Database Management Systems (DBMSs), where applicable.	5		AST-28.1			
ISM-1250	Restricting privileges for server applications	The user accounts under which server applications run have limited access to their underlying server's file system.	Functional	Intersects With	Database Management System (DBMS)	AST-35	Mechanisms exist to implement and maintain Database Management Systems (DBMSs), where applicable.	5		AST-28.1			
ISM-1255	Protecting database contents	Database users' ability to access, insert, modify and remove database contents is restricted based on their work duties.	Functional	Intersects With	Database Administrative Processes	OPS-04.2	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	5		AST-28			
ISM-1256	Protecting databases	File-based access controls are applied to database files.	Functional	Intersects With	Database Administrative Processes	OPS-04.2	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	5		AST-28			
ISM-1260	Hardening server application configurations	Default user accounts or credentials for server applications, including for any pre-configured user accounts, are changed, disabled or removed during initial setup.	Functional	Intersects With	Database Management System (DBMS)	AST-35	Mechanisms exist to implement and maintain Database Management Systems (DBMSs), where applicable.	5		AST-28.1			
ISM-1263	Privileged access to systems	Unique privileged user accounts are used for administering individual server applications.	Functional	Intersects With	Database Management System (DBMS)	AST-35	Mechanisms exist to implement and maintain Database Management Systems (DBMSs), where applicable.	5		AST-28.1			
ISM-1268	Protecting database contents	The need-to-know principle is enforced for database contents through the application of minimum privileges, database views, database roles and data tokenisation.	Functional	Intersects With	Database Administrative Processes	OPS-04.2	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	5		AST-28			
ISM-1269	Functional separation between database servers and web servers	Database servers and web servers are functionally separated.	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network resources.	5		NET-06			
ISM-1269	Functional separation between database servers and web servers	Database servers and web servers are functionally separated.	Functional	Intersects With	Microsegmentation	NET-11	Automated mechanisms exist to enable microsegmentation, either physically or virtually, to divide the network according to application and data workflows communications needs.	5		NET-06.6			
ISM-1269	Functional separation between database servers and web servers	Database servers and web servers are functionally separated.	Functional	Intersects With	Database Administrative Processes	OPS-04.2	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	5		AST-28			
ISM-1270	Network environment	Database servers are placed on a different network segment to user workstations.	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network resources.	5		NET-06			
ISM-1270	Network environment	Database servers are placed on a different network segment to user workstations.	Functional	Intersects With	Microsegmentation	NET-11	Automated mechanisms exist to enable microsegmentation, either physically or virtually, to divide the network according to application and data workflows communications needs.	5		NET-06.6			
ISM-1270	Network environment	Database servers are placed on a different network segment to user workstations.	Functional	Intersects With	Database Administrative Processes	OPS-04.2	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	5		AST-28			
ISM-1271	Network environment	Network access controls are implemented to restrict database server communications to strictly defined network resources that require access to the database server.	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network resources.	5		NET-06			
ISM-1271	Network environment	Network access controls are implemented to restrict database server communications to strictly defined network resources that require access to the database server.	Functional	Intersects With	Microsegmentation	NET-11	Automated mechanisms exist to enable microsegmentation, either physically or virtually, to divide the network according to application and data workflows communications needs.	5		NET-06.6			
ISM-1271	Network environment	Network access controls are implemented to restrict database server communications to strictly defined network resources that require access to the database server.	Functional	Intersects With	Database Administrative Processes	OPS-04.2	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	5		AST-28			
ISM-1272	Network environment	If only local access to a database is required, networking functionality of database management system applications is disabled or directed to listen solely to the localhost interface.	Functional	Intersects With	Database Administrative Processes	OPS-04.2	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	5		AST-28			
ISM-1273	Segregation of development, testing, staging and production database servers	Database servers for development, testing, staging and production environments are segregated.	Functional	Intersects With	Database Administrative Processes	OPS-04.2	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	5		AST-28			
ISM-1273	Segregation of development, testing, staging and production database servers	Database servers for development, testing, staging and production environments are segregated.	Functional	Intersects With	Separation of Development, Testing and Operational Environments	TDA-15.1	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 Technology Assets, Applications and/or Services (TAAS).	5		TDA-08			
ISM-1274	Segregation of development, testing, staging and production databases	Database contents from production environments are not used in non-production environments unless the non-production environment is secured to at least the same level as the production environment.	Functional	Intersects With	Database Administrative Processes	OPS-04.2	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	5		AST-28			
ISM-1274	Segregation of development, testing, staging and production databases	Database contents from production environments are not used in non-production environments unless the non-production environment is secured to at least the same level as the production environment.	Functional	Intersects With	Separation of Development, Testing and Operational Environments	TDA-15.1	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 Technology Assets, Applications and/or Services (TAAS).	5		TDA-08			
ISM-1275	Software interaction with databases	All queries to databases from software are filtered for legitimate content and correct syntax.	Functional	Intersects With	DNS & Content Filtering	NET-17	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		NET-18			
ISM-1275	Software interaction with databases	All queries to databases from software are filtered for legitimate content and correct syntax.	Functional	Intersects With	Database Administrative Processes	OPS-04.2	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	5		AST-28			
ISM-1276	Software interaction with databases	Parameterised queries or stored procedures, instead of dynamically generated queries, are used by software for database interactions.	Functional	Intersects With	Database Administrative Processes	OPS-04.2	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	5		AST-28			
ISM-1277	Communications between database servers and web servers	Data communicated between database servers and web servers is encrypted using Australian Signals Directorate-approved cryptography.	Functional	Intersects With	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5		CRY-01			
ISM-1277	Communications between database servers and web servers	Data communicated between database servers and web servers is encrypted using Australian Signals Directorate-approved cryptography.	Functional	Intersects With	Database Encryption	CRY-08	Mechanisms exist to ensure that database servers utilize encryption to protect the confidentiality of the data within the databases.	5		CRY-05.3			
ISM-1277	Communications between database servers and web servers	Data communicated between database servers and web servers is encrypted using Australian Signals Directorate-approved cryptography.	Functional	Intersects With	Database Administrative Processes	OPS-04.2	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	5		AST-28			
ISM-1278	Software interaction with databases	Software is designed or configured to provide as little error information as possible about the structure of databases.	Functional	Intersects With	Database Administrative Processes	OPS-04.2	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	5		AST-28			
ISM-1284	Content validation	Files imported or exported via gateways or CDSs undergo content validation.	Functional	Intersects With	Malicious Code Protection (Antimalware)	END-04	Mechanisms exist to utilize antimalware, or similar technologies, to detect and eradicate malicious code.	5		END-04			
ISM-1284	Content validation	Files imported or exported via gateways or CDSs undergo content validation.	Functional	Intersects With	Heuristic / Nonsignature-Based Malware Detection	END-04.2	Mechanisms exist to utilize heuristic / nonsignature-based antimalware detection capabilities.	5		END-04.4			
ISM-1284	Content validation	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		NET-03			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-1286	Content conversion	Files imported or exported via gateways or CDSs undergo content conversion.	Functional	Intersects With	Malicious Code Protection (Antimalware)	END-04	Mechanisms exist to utilize antimalware, or similar technologies, to detect and eradicate malicious code.	5		END-04			
ISM-1286	Content conversion	Files imported or exported via gateways or CDSs undergo content conversion.	Functional	Intersects With	Heuristic / Nonsignature-Based Malware Detection	END-04.2	Mechanisms exist to utilize heuristic / nonsignature-based antimalware detection capabilities.	5		END-04.4			
ISM-1286	Content conversion	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		NET-03			
ISM-1287	Content sanitisation	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		NET-03			
ISM-1287	Content sanitisation	Files imported or exported via gateways or CDSs undergo content sanitisation.	Functional	Intersects With	DNS & Content Filtering	NET-17	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		NET-18			
ISM-1287	Content sanitisation	Files imported or exported via gateways or CDSs undergo content sanitisation.	Functional	Intersects With	Cross Domain Solution (CDS)	NET-41	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	5		NET-02.3			
ISM-1288	Antivirus scanning	Files imported or exported via gateways or CDSs undergo antivirus scanning using multiple different scanning engines.	Functional	Intersects With	Malicious Code Protection (Antimalware)	END-04	Mechanisms exist to utilize antimalware, or similar technologies, to detect and eradicate malicious code.	5		END-04			
ISM-1288	Antivirus scanning	Files imported or exported via gateways or CDSs undergo antivirus scanning using multiple different scanning engines.	Functional	Intersects With	Heuristic / Nonsignature-Based Malware Detection	END-04.2	Mechanisms exist to utilize heuristic / nonsignature-based antimalware detection capabilities.	5		END-04.4			
ISM-1288	Antivirus scanning	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		NET-03			
ISM-1289	Archive files	Archive files imported or exported via gateways or CDSs are unpacked to undergo content filtering checks.	Functional	Intersects With	Malicious Code Protection (Antimalware)	END-04	Mechanisms exist to utilize antimalware, or similar technologies, to detect and eradicate malicious code.	5		END-04			
ISM-1289	Archive files	Archive files imported or exported via gateways or CDSs are unpacked to undergo content filtering checks.	Functional	Intersects With	Heuristic / Nonsignature-Based Malware Detection	END-04.2	Mechanisms exist to utilize heuristic / nonsignature-based antimalware detection capabilities.	5		END-04.4			
ISM-1289	Archive files	Archive files imported or exported via gateways or CDSs are unpacked 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		NET-03			
ISM-1290	Archive files	Archive files are unpacked in a controlled manner to ensure content filter performance or availability is not adversely affected.	Functional	Intersects With	Malicious Code Protection (Antimalware)	END-04	Mechanisms exist to utilize antimalware, or similar technologies, to detect and eradicate malicious code.	5		END-04			
ISM-1293	Encrypted files	Encrypted files imported or exported via gateways or CDSs are decrypted to undergo content filtering checks.	Functional	Intersects With	Malicious Code Protection (Antimalware)	END-04	Mechanisms exist to utilize antimalware, or similar technologies, to detect and eradicate malicious code.	5		END-04			
ISM-1293	Encrypted files	Encrypted files imported or exported via gateways or CDSs are decrypted to undergo content filtering checks.	Functional	Intersects With	Heuristic / Nonsignature-Based Malware Detection	END-04.2	Mechanisms exist to utilize heuristic / nonsignature-based antimalware detection capabilities.	5		END-04.4			
ISM-1293	Encrypted files	Encrypted files imported or exported via gateways or CDSs are decrypted 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		NET-03			
ISM-1293	Encrypted files	Encrypted files imported or exported via gateways or CDSs are decrypted to undergo content filtering checks.	Functional	Intersects With	DNS & Content Filtering	NET-17	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		NET-18			
ISM-1294	Monitoring data import and export	Data transfer logs for systems are partially verified at least monthly.	Functional	Subset Of	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10		MON-01			
ISM-1294	Monitoring data import and export	Data transfer logs for systems are partially verified at least monthly.	Functional	Intersects With	Analyze and Prioritize Monitoring Requirements	MON-03.2	Mechanisms exist to assess the organization's needs for monitoring and prioritize the monitoring of Technology Assets, Applications and/or Services (TAAS), based on TAAS criticality and the sensitivity of the data it stores, transmits and processes.	5		MON-01.16			
ISM-1296	Physical access to network devices in public areas	Physical security is implemented to protect network devices in public areas from physical damage or unauthorised access.	Functional	Intersects With	Physical Access Control	PES-08	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).	5		PES-03			
ISM-1297	Privately owned mobile devices and desktop computers	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-27	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		AST-16			
ISM-1297	Privately owned mobile devices and desktop computers	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-02	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	10		MDM-01			
ISM-1297	Privately owned mobile devices and desktop computers	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 Technology Assets, Applications and/or Services (TAAS).	5		MDM-06			
ISM-1298	Before travelling overseas with mobile devices	Personnel are advised of privacy and security risks when travelling overseas with mobile devices.	Functional	Intersects With	Travel-Only Devices	AST-32	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		AST-24			
ISM-1299	Personnel awareness	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	Intersects With	Travel-Only Devices	AST-32	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		AST-24			
ISM-1300	After travelling overseas with mobile devices	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-32	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		AST-24			
ISM-1300	After travelling overseas with mobile devices	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-33	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		AST-25			
ISM-1300	After travelling overseas with mobile devices	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	Digital Media Sanitization	DCH-18	Mechanisms exist to sanitize digital 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		DCH-09			
ISM-1304	Default user accounts and credentials for network devices	Default user accounts or credentials for network devices, including for any pre-configured user accounts, are changed, disabled or removed during initial setup.	Functional	Intersects With	Default Authenticators	IAC-14.4	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	5		IAC-10.8			
ISM-1311	Using the Simple Network Management Protocol	SNMP version 1 and SNMP version 2 are not used on networks.	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5		CFG-03			
ISM-1312	Using the Simple Network Management Protocol	All default SNMP community strings on network devices are changed and write access is disabled.	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5		CFG-03			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-1314	Choosing wireless devices	All wireless devices are Wi-Fi Alliance certified.	Functional	Intersects With	Wireless Access Authentication & Encryption	CFG-04.8	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5		CRY-07			
ISM-1314	Choosing wireless devices	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 Technology Assets, Applications and/or Services (TAAS).	5		NET-03.1			
ISM-1314	Choosing wireless devices	All wireless devices are Wi-Fi Alliance certified.	Functional	Intersects With	Wireless Networking	NET-24	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5		NET-15			
ISM-1315	Administrative interfaces for wireless access points	The administrative interface on wireless access points is disabled for wireless network connections.	Functional	Intersects With	Wireless Networking	NET-24	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5		NET-15			
ISM-1316	Default settings	Default SSIDs of wireless access points are changed.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1316	Default settings	Default SSIDs of wireless access points are changed.	Functional	Intersects With	Wireless Networking	NET-24	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5		NET-15			
ISM-1317	Default settings	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	Intersects With	Wireless Networking	NET-24	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5		NET-15			
ISM-1318	Default settings	SSID broadcasting is not disabled on wireless access points.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1318	Default settings	SSID broadcasting is not disabled on wireless access points.	Functional	Intersects With	Wireless Networking	NET-24	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5		NET-15			
ISM-1319	Static addressing	Static addressing is not used for assigning IP addresses on wireless networks.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1319	Static addressing	Static addressing is not used for assigning IP addresses on wireless networks.	Functional	Intersects With	Wireless Networking	NET-24	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5		NET-15			
ISM-1320	Media Access Control address filtering	MAC address filtering is not used to restrict which devices can connect to wireless networks.	Functional	Intersects With	Wireless Networking	NET-24	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5		NET-15			
ISM-1321	802.1X authentication	802.1X authentication with EAP-TLS, using X.509 certificates, is used for mutual authentication; with all other EAP methods disabled on supplicants and authentication servers.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1321	802.1X authentication	802.1X authentication with EAP-TLS, using X.509 certificates, is used for mutual authentication; with all other EAP methods disabled on supplicants and authentication servers.	Functional	Intersects With	Wireless Networking	NET-24	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5		NET-15			
ISM-1322	Evaluation of 802.1X authentication implementation	Evaluated supplicants, authenticators, wireless access points and authentication servers are used in wireless networks.	Functional	Intersects With	Wireless Networking	NET-24	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5		NET-15			
ISM-1323	Generating and issuing certificates for authentication	Certificates are required for devices and users accessing wireless networks.	Functional	Intersects With	Wireless Networking	NET-24	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5		NET-15			
ISM-1324	Generating and issuing certificates for authentication	Certificates are generated using an evaluated certificate authority or hardware security module.	Functional	Intersects With	Wireless Networking	NET-24	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5		NET-15			
ISM-1327	Generating and issuing certificates for authentication	Certificates are protected by logical and physical access controls, encryption, and user authentication.	Functional	Intersects With	Wireless Networking	NET-24	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5		NET-15			
ISM-1330	Caching 802.1X authentication outcomes	The PMK caching period is not set to greater than 1440 minutes (24 hours).	Functional	Intersects With	Wireless Networking	NET-24	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5		NET-15			
ISM-1332	Confidentiality and integrity of wireless network traffic	WPA3-Enterprise 192-bit mode is used to protect the confidentiality and integrity of all wireless network traffic.	Functional	Intersects With	Wireless Access Authentication & Encryption	CFG-04.8	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5		CRY-07			
ISM-1334	Interference between wireless networks	Wireless networks implement sufficient frequency separation from other wireless networks.	Functional	Intersects With	Wireless Networking	NET-24	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5		NET-15			
ISM-1335	Protecting management frames on wireless networks	Wireless access points enable the use of the 802.11w amendment to protect management frames.	Functional	Intersects With	Wireless Networking	NET-24	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5		NET-15			
ISM-1338	Wireless network footprint	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	Intersects With	Wireless Boundaries	NET-24.2	Mechanisms exist to confine wireless communications to organization-controlled boundaries.	5		NET-15.4			
ISM-1341	Host-based intrusion detection and response solution	A HIPS or EDR solution is implemented on workstations.	Functional	Intersects With	Endpoint Detection & Response (EDR)	END-09	Mechanisms exist to utilize Endpoint Detection & Response (EDR) capabilities to detect, investigate and respond to anomalous and/or malicious activity.	8	Updated 2026.3	END-06.2			
ISM-1341	Host-based intrusion detection and response solution	A HIPS or EDR solution is implemented on workstations.	Functional	Intersects With	Host Intrusion Detection and Prevention Systems (HIDS / HIPS)	END-12	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	5		END-07			
ISM-1359	Removable media usage policy	A removable media usage policy is developed, implemented and maintained.	Functional	Intersects With	Removable Media Security	DCH-21	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	5		DCH-12			
ISM-1361	Media destruction equipment	Security Construction and Equipment Committee-approved equipment or ASIO-approved equipment is used when destroying media.	Functional	Intersects With	Digital & Non-Digital Media Disposal	DCH-17	Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.	5		DCH-08			
ISM-1364	Using Virtual Local Area Networks	Network devices managing VLANs terminate VLANs belonging to different security domains on separate physical network interfaces.	Functional	Intersects With	Virtual Local Area Network (VLAN) Separation	NET-10	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.	5		NET-06.2			
ISM-1366	Maintaining mobile device security	Security updates are applied to mobile devices as soon as they become available.	Functional	Intersects With	Use of Mobile Devices	HRS-06.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5		HRS-05.5			
ISM-1366	Maintaining mobile device security	Security updates are applied to mobile devices as soon as they become available.	Functional	Subset Of	Centralized Management Of Mobile Devices	MDM-02	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	10		MDM-01			
ISM-1369	Configuring Transport Layer Security	AES-GCM is used for encryption of TLS connections.	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03			
ISM-1370	Configuring Transport Layer Security	Only server-initiated secure renegotiation is used for TLS connections.	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03			
ISM-1372	Configuring Transport Layer Security	DH or ECDH is used for key establishment of TLS connections.	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03			
ISM-1373	Configuring Transport Layer Security	Anonymous DH is not used for TLS connections.	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03			
ISM-1374	Configuring Transport Layer Security	SHA-2-based certificates are used for TLS connections.	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03			
ISM-1375	Configuring Transport Layer Security	SHA-2 is used for the Hash-based Message Authentication Code (HMAC) and pseudorandom function (PRF) for TLS connections.	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03			
ISM-1380	Separate privileged operating environments	Privileged users use separate privileged and unprivileged operating environments.	Functional	Intersects With	Dedicated Privileged Account	IAC-10.3	Mechanisms exist to assign dedicated privileged user accounts to be used solely for duties requiring privileged access.	5	Updated 2026.3	IAC-16.4	ML1	ML2	ML3
ISM-1380	Separate privileged operating environments	Privileged users use separate privileged and unprivileged operating environments.	Functional	Intersects With	Non-Privileged Access for Non-Security Functions	IAC-30.3	Mechanisms exist to prohibit privileged users from using privileged accounts, while performing non-security functions.	8	Updated 2026.3	IAC-21.2	ML1	ML2	ML3
ISM-1380	Separate privileged operating environments	Privileged users use separate privileged and unprivileged operating environments.	Functional	Intersects With	System Administrative Processes	OPS-04.1	Mechanisms exist to develop, implement and govern system administration processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining Technology Assets, Applications and/or Services (TAAS).	3	Updated 2026.3	AST-26	ML1	ML2	ML3
ISM-1385	Administrative infrastructure	Administrative infrastructure is segregated from the wider network and the internet.	Functional	Intersects With	Jump Server	AST-34	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		AST-27			
ISM-1385	Administrative infrastructure	Administrative infrastructure is segregated from the wider network and the internet.	Functional	Intersects With	Cloud Infrastructure Security Subnet	CLD-06	Mechanisms exist to host security-specific technologies in a dedicated subnet.	5		CLD-03			
ISM-1385	Administrative infrastructure	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		NET-06.1			
ISM-1385	Administrative infrastructure	Administrative infrastructure is segregated from the wider network and the internet.	Functional	Intersects With	Segregation From Enterprise Services	NET-08.2	Mechanisms exist to isolate sensitive and/or regulated data enclaves (secure zones) from corporate-provided IT resources by providing enclave-specific IT services (e.g., directory services, DNS, NTP, ITAM, antimalware and patch management) to those isolated network segments.	5		NET-06.4			
ISM-1385	Administrative infrastructure	Administrative infrastructure is segregated from the wider network and the internet.	Functional	Intersects With	System Administrative Processes	OPS-04.1	Mechanisms exist to develop, implement and govern system administration processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining Technology Assets, Applications and/or Services (TAAS).	5		AST-26			
ISM-1386	Administrative infrastructure	Network management traffic can only originate from administrative infrastructure.	Functional	Intersects With	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.	5		NET-04			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-1387	Administrative infrastructure	Administrative activities are conducted through jump servers.	Functional	Equal	Jump Server	AST-34	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	Updated 2026.3	AST-27		ML2	ML3
ISM-1389	Automated dynamic analysis	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-21	Mechanisms exist to utilize a detonation chamber capability to detect and/or block potentially-malicious files and email attachments.	5		IRO-15			
ISM-1389	Automated dynamic analysis	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		NET-03			
ISM-1392	Application control	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 Technology Assets, Applications and/or Services (TAAS) to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5		CFG-03			
ISM-1392	Application control	When implementing application control using path rules, only approved users can modify approved files and write to approved folders.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-14.1	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5	Updated 2026.3	CFG-03.3			
ISM-1392	Application control	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-30	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		IAC-21			
ISM-1395	Contractual security requirements with service providers	Service providers, including any subcontractors, provide an appropriate level of protection for any data entrusted to them or their services.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-05			
ISM-1400	Privately owned mobile devices and desktop computers	Personnel using privately owned mobile devices or desktop computers to access OFFICIAL: Sensitive or PROTECTED systems or data have enforced separation of classified data and personal data.	Functional	Intersects With	Personally-Owned Mobile Devices	MDM-06	Mechanisms exist to restrict the connection of personally-owned, mobile devices to organizational Technology Assets, Applications and/or Services (TAAS).	5		MDM-06			
ISM-1401	Multi-factor authentication	Multi-factor authentication uses either: something users have and something users know, or something users have that is unlocked by something users know or are.	Functional	Subset Of	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	10	Updated 2026.3	IAC-06	ML1	ML2	ML3
ISM-1402	Protecting credentials	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	Intersects With	Protection of Authenticators	IAC-14.2	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	5		IAC-10.5			
ISM-1403	User account lockouts	User accounts, except for break glass accounts, are protected by fixed or risk-based lockout mechanisms aligned to a maximum of five failed logon attempts, with either indefinite or automated lockout durations.	Functional	Intersects With	Account Lockout	CFG-04.1	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.	5		IAC-22			
ISM-1404	Suspension of access to systems	Unprivileged access to systems and their resources are disabled after 45 days of inactivity.	Functional	Intersects With	Disable Inactive Accounts	IAC-08.4	Automated mechanisms exist to disable inactive accounts after an organization-defined time period.	5		IAC-15.3			
ISM-1405	Centralised event logging facility	A centralised event logging facility is implemented.	Functional	Intersects With	Centralized Collection of Event Logs & Security-Relevant Telemetry	MON-05	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of event logs and security-relevant telemetry.	5		MON-02			
ISM-1406	Standard Operating Environments	SOEs are used for workstations and servers.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1407	Operating system releases and versions	The latest release, or the previous release, of operating systems are used.	Functional	Intersects With	Stable Versions	AST-37.1	Mechanisms exist to install the latest stable version of any software and/or security-related updates on all applicable systems.	5	Updated 2026.3	VPM-04.1			ML3
ISM-1407	Operating system releases and versions	The latest release, or the previous release, of operating systems are used.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5	Updated 2026.3	CFG-02			ML3
ISM-1408	Operating system releases and versions	Where supported, 64-bit versions of operating systems are used.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1409	Hardening operating system configurations	Operating systems are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1412	Web browsers	Web browsers are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5	Updated 2026.3	CFG-02		ML2	ML3
ISM-1416	Software firewall	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	Intersects With	Software Firewall	END-07	Mechanisms exist to utilize host-based firewall software, or a similar technology, on all endpoint devices, where technically feasible.	5		END-05			
ISM-1417	Antivirus application	An antivirus application 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 at least daily • regular scanning configured for all fixed disks and removable media.	Functional	Intersects With	Malicious Code Protection (Antimalware)	END-04	Mechanisms exist to utilize antimalware, or similar technologies, to detect and eradicate malicious code.	5		END-04			
ISM-1417	Antivirus application	An antivirus application 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 at least daily • regular scanning configured for all fixed disks and removable media.	Functional	Intersects With	Heuristic / Nonsignature-Based Malware Detection	END-04.2	Mechanisms exist to utilize heuristic / nonsignature-based antimalware detection capabilities.	5		END-04.4			
ISM-1418	Device access control	If there is no business requirement for reading from removable media and devices, such functionality is disabled via the use of a device access control application or by disabling external communication interfaces.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1418	Device access control	If there is no business requirement for reading from removable media and devices, such functionality is disabled via the use of a device access control application or by disabling external communication interfaces.	Functional	Intersects With	Host Intrusion Detection and Prevention Systems (HIDS / HIPS)	END-12	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		END-07			
ISM-1419	Development, testing, staging and production environments	Development and modification of software only take place in development environments.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-05	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5		TDA-06			
ISM-1419	Development, testing, staging and production environments	Development and modification of software only take place in development environments.	Functional	Intersects With	Secure Development Environments	TDA-15	Mechanisms exist to maintain a segmented development network to ensure a secure development environment.	5		TDA-07			
ISM-1420	Development, testing, staging and production environments	Data from production environments is not used in non-production environments unless the non-production environment is secured to at least the same level as the production environment.	Functional	Intersects With	Use of Live Data	TDA-18	Mechanisms exist to approve, document and control the use of live data in development and test environments.	5		TDA-10			
ISM-1422	Authoritative source for software	Unauthorised access to the authoritative source for software is prevented.	Functional	Intersects With	Access to Program Source Code	TDA-16.1	Mechanisms exist to limit privileges to change software resident within software libraries.	5		TDA-20			
ISM-1424	Web security policy response headers	Content-Security-Policy, Hypertext Transfer Protocol Strict Transport Security and X-Frame-Options are specified by web server software via security policy in response headers.	Functional	Intersects With	Web Browser Security	WEB-11	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.	5		WEB-12			
ISM-1427	Implementing gateways	Gateways perform ingress traffic filtering to detect and prevent IP source address spoofing.	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		NET-03			
ISM-1428	Using Internet Protocol version 6	Unless explicitly required, IPv6 tunnelling is disabled on all network devices.	Functional	Subset Of	Network Security Controls (NSC)	NET-02	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10		NET-01			
ISM-1429	Using Internet Protocol version 6	IPv6 tunnelling is blocked by network security appliances at externally connected network boundaries.	Functional	Subset Of	Network Security Controls (NSC)	NET-02	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10		NET-01			
ISM-1430	Using Internet Protocol version 6	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-02	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10		NET-01			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-1431	Denial-of-service attack mitigation strategies	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	Intersects With	Denial of Service (DoS) Protection	NET-21	Automated mechanisms exist to protect against or limit the effects of denial of service attacks.	5		NET-02.1			
ISM-1432	Denial-of-service attack mitigation strategies	Domain names for online services are protected via registrar locking and confirming that domain registration details are correct.	Functional	Intersects With	Domain Registrar Security	NET-13.3	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.	5		NET-10.4			
ISM-1436	Denial-of-service attack mitigation strategies	Critical online services are segregated from other online services that are more likely to be targeted as part of denial-of-service attacks.	Functional	Intersects With	Denial of Service (DoS) Protection	NET-21	Automated mechanisms exist to protect against or limit the effects of denial of service attacks.	5		NET-02.1			
ISM-1437	Cloud-based hosting of online services	Cloud service providers are used for hosting online services.	Functional	Subset Of	Cloud Services	CLD-02	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	10		CLD-01			
ISM-1438	Using content delivery networks	Where a high availability requirement exists for website hosting, CDNs that cache websites are used.	Functional	Intersects With	Side Channel Attack Prevention	NET-47	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.	5		CLD-12			
ISM-1439	Using content delivery networks	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	Intersects With	Side Channel Attack Prevention	NET-47	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.	5		CLD-12			
ISM-1446	Using Elliptic Curve Cryptography	When using elliptic curve cryptography, a suitable curve from NIST SP 800-186 is used.	Functional	Subset Of	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		CRY-01			
ISM-1448	Configuring Transport Layer Security	When using DH or ECDH for key establishment of TLS connections, the ephemeral variant is used.	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03			
ISM-1449	Authentication mechanisms	SSH private keys are protected with a password or a key encryption key.	Functional	Intersects With	Public Key Infrastructure (PKI)	CRY-09	Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service provider.	5		CRY-08			
ISM-1450	Microphones and webcams	Microphones (including headsets and USB handsets) and webcams are not used with non-TOP SECRET workstations in TOP SECRET areas.	Functional	Intersects With	Microphones & Web Cameras	CFG-04.11	Mechanisms exist to configure assets to prohibit the use of endpoint-based microphones and web cameras in secure areas or where sensitive and/or regulated information is discussed.	5		AST-22			
ISM-1451	Contractual security requirements with service providers	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-08	Mechanisms exist to protect sensitive and/or regulated data that is collected, developed, received, transmitted, used or stored in support of the performance of a contract.	5		IAO-03.2			
ISM-1451	Contractual security requirements with service providers	Types of data and its ownership is documented in contractual arrangements with service providers.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-05			
ISM-1452	Cyber supply chain risk management activities	A supply chain risk assessment is performed for suppliers of operating systems, applications, IT equipment, OT equipment and services to assess the impact to a system's security risk profile.	Functional	Intersects With	Supply Chain Risk Assessment (SCRA)	RSK-21	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	5		RSK-09.1			
ISM-1452	Cyber supply chain risk management activities	A supply chain risk assessment is performed for suppliers of operating systems, applications, IT equipment, OT equipment and services to assess the impact to a system's security risk profile.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-04	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5		TPM-03			
ISM-1452	Cyber supply chain risk management activities	A supply chain risk assessment is performed for suppliers of operating systems, applications, IT equipment, OT equipment and services to assess the impact to a system's security risk profile.	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5		TPM-02			
ISM-1453	Configuring Transport Layer Security	Perfect Forward Secrecy (PFS) is used for TLS connections.	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03			
ISM-1454	Remote Authentication Dial-In User Service authentication	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	Intersects With	Wireless Networking	NET-24	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5		NET-15			
ISM-1457	Using peripheral switches	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-02	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10		AST-01			
ISM-1460	Functional separation between operating environments	When using a software-based isolation mechanism that consumes shared physical computing resources, the isolation mechanism is from a vendor that has demonstrated a commitment to Secure by Design and Secure by Default principles and practices, including secure programming practices and either memory-safe programming languages or less preferably memory-safe programming practices.	Functional	Intersects With	Virtualization Techniques	SEA-23	Mechanisms exist to utilize virtualization techniques to support the employment of a diversity of operating systems and applications.	5		SEA-13.1			
ISM-1461	Functional separation between operating environments	When using a software-based isolation mechanism that consumes shared physical computing resources for SECRET or TOP SECRET operating environments, the physical server and all operating environments are of the same classification and belong to the same security domain.	Functional	Intersects With	Virtualization Techniques	SEA-23	Mechanisms exist to utilize virtualization techniques to support the employment of a diversity of operating systems and applications.	5		SEA-13.1			
ISM-1467	User application releases	The latest release of email clients, office productivity suites, PDF applications, security products and web browsers, including their extensions, are used.	Functional	Intersects With	Stable Versions	AST-37.1	Mechanisms exist to install the latest stable version of any software and/or security-related updates on all applicable systems.	5		VPM-04.1			
ISM-1467	User application releases	The latest release of email clients, office productivity suites, PDF applications, security products and web browsers, including their extensions, are used.	Functional	Intersects With	Automated Software & Firmware Updates	VPM-08.1	Automated mechanisms exist to install the latest stable versions of security-relevant software and firmware updates.	5		VPM-05.4			
ISM-1470	Hardening user application configurations	Unneeded user accounts, components, services and functionality of user applications are disabled or removed.	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5		CFG-03			
ISM-1471	Application control	When implementing application control using publisher certificate rules, publisher names and product names are used.	Functional	Intersects With	Integrity Assurance & Enforcement (IAE)	CFG-08.2	Automated mechanisms exist to: (1) Identify unauthorized deviations from an approved secure baseline configuration; and (2) Implement automated resiliency actions to remediate the unauthorized change.	5	Updated 2026.3	CFG-06			
ISM-1478	Overseeing the cyber security program	The CISO oversees their organisation's cyber security program and ensures their organisation's compliance with cyber security policy, standards, regulations and legislation.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8		GOV-02			
ISM-1479	Functional separation between servers	Servers minimise communications with other servers at the network and file system level.	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5		CFG-03			
ISM-1480	Using peripheral switches	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-02	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10		AST-01			
ISM-1482	Organisation-owned mobile devices and desktop computers	Personnel using organisation-owned mobile devices or desktop computers to access classified systems or data have enforced separation of classified data and personal data.	Functional	Intersects With	Personally-Owned Mobile Devices	MDM-06	Mechanisms exist to restrict the connection of personally-owned, mobile devices to organizational Technology Assets, Applications and/or Services (TAAS).	5		MDM-06			
ISM-1483	Server application releases	The latest release of internet-facing server applications is used.	Functional	Intersects With	Stable Versions	AST-37.1	Mechanisms exist to install the latest stable version of any software and/or security-related updates on all applicable systems.	5		VPM-04.1			
ISM-1485	Web browsers	Web browsers do not process web advertisements from the internet.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5	Updated 2026.3	CFG-02	ML1	ML2	ML3
ISM-1486	Web browsers	Web browsers do not process Java from the internet.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5	Updated 2026.3	CFG-02	ML1	ML2	ML3
ISM-1487	Office productivity suites	Only privileged users responsible for checking that Microsoft Office macros are free of malicious code can write to and modify content within Trusted Locations.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5	Updated 2026.3	CFG-02			ML3
ISM-1488	Office productivity suites	Microsoft Office macros in files originating from the internet are blocked.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5	Updated 2026.3	CFG-02	ML1	ML2	ML3
ISM-1489	Office productivity suites	Microsoft Office macro security settings cannot be changed by users.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5	Updated 2026.3	CFG-02	ML1	ML2	ML3

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-1490	Application control	Application control is implemented on internet-facing servers.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5	Updated 2026.3	CFG-02		ML2	ML3
ISM-1491	Hardening operating system configurations	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	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1492	Hardening operating system configurations	Operating system exploit protection functionality is enabled.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1493	Software registers	Software registers for workstations, servers, network devices and networked IT equipment are developed, implemented, maintained and regularly verified.	Functional	Intersects With	Configuration Management Database (CMDB)	AST-08.1	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	5		AST-02.9			
ISM-1493	Software registers	Software registers for workstations, servers, network devices and networked IT equipment are developed, implemented, maintained and regularly verified.	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		VPM-05			
ISM-1501	Cessation of support	Operating systems that are no longer supported by vendors are replaced.	Functional	Intersects With	Unsupported Technology Assets, Applications and/or Services (TAAS)	AST-39	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs.	5		TDA-17	ML1	ML2	ML3
ISM-1502	Blocking suspicious emails	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	Intersects With	DNS & Content Filtering	NET-17	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		NET-18			
ISM-1504	Multi-factor authentication	Multi-factor authentication is used to authenticate users to their organisation's online services that process, store or communicate their organisation's sensitive data.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5		IAC-06	ML1	ML2	ML3
ISM-1505	Multi-factor authentication	Multi-factor authentication is used to authenticate users of data repositories.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5		IAC-06			ML3
ISM-1506	Configuring Secure Shell	The use of SSH version 1 is disabled for SSH connections.	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03			
ISM-1507	Privileged access to systems	Requests for privileged access to systems and their resources are validated when first requested.	Functional	Intersects With	Management Approval For New or Changed Accounts	IAC-09	Mechanisms exist to ensure management approvals are required for new accounts or changes in permissions to existing accounts.	5	Updated 2026.3	IAC-28.1			
ISM-1507	Privileged access to systems	Requests for privileged access to systems and their resources are validated when first requested.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-10	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5	Updated 2026.3	IAC-16			
ISM-1508	Privileged access to systems	Privileged access to systems and their resources is limited to only what is required for users and services to undertake their duties.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-10	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5	Updated 2026.3	IAC-16			
ISM-1508	Privileged access to systems	Privileged access to systems and their resources is limited to only what is required for users and services to undertake their duties.	Functional	Intersects With	Least Privilege	IAC-30	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	Updated 2026.3	IAC-21			
ISM-1509	Privileged access to systems	Privileged access events are centrally logged.	Functional	Intersects With	Centralized Collection of Event Logs & Security-Relevant Telemetry	MON-05	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of event logs and security-relevant telemetry.	8	Updated 2026.3	MON-02			
ISM-1509	Privileged access to systems	Privileged access events are centrally logged.	Functional	Intersects With	Privileged Functions Logging	MON-14	Mechanisms exist to log and review the actions of users and/or services with elevated privileges.	8	Updated 2026.3	MON-03.3			
ISM-1510	Digital preservation policy	A digital preservation policy is developed, implemented and maintained.	Functional	Intersects With	Retention Of Previous Configurations	CFG-09	Mechanisms exist to retain previous versions of secure baseline configuration to support roll back.	5		CFG-02.3			
ISM-1510	Digital preservation policy	A digital preservation policy is developed, implemented and maintained.	Functional	Intersects With	Media & Data Retention	DCH-27	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5		DCH-18			
ISM-1511	Performing and retaining backups	Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements.	Functional	Intersects With	Data Backups	BCD-24	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	8	Updated 2026.3	BCD-11	ML1	ML2	ML3
ISM-1515	Testing restoration of backups	Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises.	Functional	Intersects With	Testing for Reliability & Integrity	BCD-32	Mechanisms exist to routinely test data backups to verify the reliability of the backup process, as well as the integrity and availability of the data.	5		BCD-11.1	ML1	ML2	ML3
ISM-1515	Testing restoration of backups	Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises.	Functional	Intersects With	Test Restoration Using Sampling	BCD-32.1	Mechanisms exist to utilize sampling of available data backups to test recovery capabilities as part of business continuity plan testing.	5	Updated 2026.3	BCD-11.5			
ISM-1517	Media destruction methods	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	Intersects With	Digital & Non-Digital Media Disposal	DCH-17	Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.	5		DCH-08			
ISM-1520	System administrators for gateways	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	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		NET-03			
ISM-1521	Separation of data flows	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		NET-03			
ISM-1521	Separation of data flows	CDSs implement protocol breaks at each network layer.	Functional	Intersects With	Cross Domain Solution (CDS)	NET-41	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	5		NET-02.3			
ISM-1522	Separation of data flows	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		NET-03			
ISM-1522	Separation of data flows	CDSs implement independent security-enforcing functions for upward and downward network paths.	Functional	Intersects With	Cross Domain Solution (CDS)	NET-41	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	5		NET-02.3			
ISM-1523	Cross Domain Solution event logging	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	Intersects With	Cross Domain Solution (CDS)	NET-41	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	5		NET-02.3			
ISM-1524	Performing content filtering	Content filters used by CDSs undergo rigorous security testing to ensure they perform as expected and cannot be bypassed.	Functional	Intersects With	DNS & Content Filtering	NET-17	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		NET-18			
ISM-1525	System ownership and oversight	System owners register each system with its authorising officer.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-02	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10		IAO-01			
ISM-1525	System ownership and oversight	System owners register each system with its authorising officer.	Functional	Intersects With	Security Authorization	IAO-14	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	5		IAO-07			
ISM-1526	Protecting systems and their resources	System owners continuously monitor the security of each system, and manage associated cyber threats, security risks and controls.	Functional	Intersects With	Monitor Controls	GOV-11.5	Mechanisms exist to compel data and/or process owners to monitor Technology Assets, Applications, Services and/or Data (TAASD) under their control on an ongoing basis for applicable threats and risks, as well as to ensure security, compliance and resilience controls are operating as intended.	5		GOV-15.5			
ISM-1526	Protecting systems and their resources	System owners continuously monitor the security of each system, and manage associated cyber threats, security risks and controls.	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5		PRM-07			
ISM-1526	Protecting systems and their resources	System owners continuously monitor the security of each system, and manage associated cyber threats, security risks and controls.	Functional	Intersects With	Risk Identification	RSK-09	Mechanisms exist to identify and document risks, both internal and external.	5		RSK-03			
ISM-1528	Using firewalls	Evaluated firewalls are used between an organisation's networks and public network infrastructure.	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		NET-03			
ISM-1529	Outsourced cloud services	Only community or private clouds are used for outsourced SECRET and TOP SECRET cloud services.	Functional	Subset Of	Cloud Services	CLD-02	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	10		CLD-01			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-1529	Outsourced cloud services	Only community or private clouds are used for outsourced SECRET and TOP SECRET cloud services.	Functional	Intersects With	Multi-Tenant Environments	CLD-07	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		CLD-06			
ISM-1530	Physical access to servers, network devices and cryptographic equipment	Classified servers, network devices and cryptographic equipment are secured in security containers suitable for their classification taking into account the combination of security zones they reside in.	Functional	Intersects With	Access To Critical Systems	PES-12	Physical access control mechanisms exist to enforce physical access to critical systems or sensitive and/or regulated data, in addition to the physical access controls for the facility.	5		PES-03.4			
ISM-1532	Using Virtual Local Area Networks	VLANs are not used to separate network traffic between an organisation's networks and public network infrastructure.	Functional	Intersects With	Virtual Local Area Network (VLAN) Separation	NET-10	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.	5		NET-06.2			
ISM-1533	Mobile device management policy	A mobile device management policy is developed, implemented and maintained.	Functional	Subset Of	Mobile Device Management Policy	MDM-01	Mechanisms exist to establish a formal, documented mobile device management policy that: (1) Conveys executive management's intent;	10	Updated 2026.3				
ISM-1533	Mobile device management policy	A mobile device management policy is developed, implemented and maintained.	Functional	Subset Of	Centralized Management Of Mobile Devices	MDM-02	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	10		MDM-01			
ISM-1534	Sanitising printers and multifunction devices	Printer ribbons in printers and MFDs are removed and destroyed.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	5		AST-09			
ISM-1535	Data transfer processes and procedures	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	Intersects With	Sensitive / Regulated Data Sharing Decisions	DCH-08.1	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	5		DCH-14			
ISM-1536	Software interaction with databases	All queries to databases from software that are initiated by users, and any resulting crash or error messages, are centrally logged.	Functional	Intersects With	Centralized Collection of Event Logs & Security-Relevant Telemetry	MON-05	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of event logs and security-relevant telemetry.	5		MON-02			
ISM-1536	Software interaction with databases	All queries to databases from software that are initiated by users, and any resulting crash or error messages, are centrally logged.	Functional	Intersects With	Content of Event Logs	MON-09	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5		MON-03			
ISM-1537	Database event logging	Security-relevant events for databases are centrally logged, including: • 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 Event Logs & Security-Relevant Telemetry	MON-05	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of event logs and security-relevant telemetry.	5		MON-02			
ISM-1537	Database event logging	Security-relevant events for databases are centrally logged, including: • 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-09	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5		MON-03			
ISM-1537	Database event logging	Security-relevant events for databases are centrally logged, including: • 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-14	Mechanisms exist to log and review the actions of users and/or services with elevated privileges.	5		MON-03.3			
ISM-1537	Database event logging	Security-relevant events for databases are centrally logged, including: • 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-32	Mechanisms exist to ensure databases produce audit records that contain sufficient information to monitor database activities.	5		MON-03.7			
ISM-1540	Domain-based Message Authentication, Reporting and Conformance	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-13	Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.	5		NET-10			
ISM-1540	Domain-based Message Authentication, Reporting and Conformance	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-39.1	Mechanisms exist to implement domain signature verification protections that authenticate incoming email according to the Domain-based Message Authentication Reporting and Conformance (DMARC).	5		NET-20.4			
ISM-1540	Domain-based Message Authentication, Reporting and Conformance	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-40.1	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5		NET-13			
ISM-1542	Office productivity suites	Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5	Updated 2026.3	CFG-02		ML2	ML3
ISM-1543	Bringing radio frequency and infrared devices into facilities	An authorised RF and IR device register for SECRET and TOP SECRET areas is developed, implemented, maintained and regularly verified.	Functional	Intersects With	Wireless Networking	NET-24	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5		NET-15			
ISM-1544	Application control	Microsoft's recommended application blocklist is implemented.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5	Updated 2026.3	CFG-02		ML2	ML3
ISM-1544	Application control	Microsoft's recommended application blocklist is implemented.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-14.1	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5		CFG-03.3		ML2	ML3
ISM-1546	Authenticating to systems	Users are authenticated before they are granted access to a system and its resources.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-02	Mechanisms exist to facilitate the implementation of Identification and Access Management (IAM) controls.	10		IAC-01			
ISM-1546	Authenticating to systems	Users are authenticated before they are granted access to a system and its resources.	Functional	Intersects With	Identification & Authentication for Organizational Users	IAC-32	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5		IAC-02			
ISM-1547	Data backup and restoration processes and procedures	Data backup processes, and supporting data backup procedures, are developed, implemented and maintained.	Functional	Intersects With	Data Backups	BCD-24	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5		BCD-11			
ISM-1548	Data backup and restoration processes and procedures	Data restoration processes, and supporting data restoration procedures, are developed, implemented and maintained.	Functional	Intersects With	Data Backups	BCD-24	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5		BCD-11			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-1549	Media management policy	A media management policy is developed, implemented and maintained.	Functional	Subset Of	Data Protection	DCH-02	Mechanisms exist to facilitate the implementation of data protection controls.	10		DCH-01			
ISM-1550	IT equipment disposal processes and procedures	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-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	5		AST-09			
ISM-1550	IT equipment disposal processes and procedures	IT equipment disposal processes, and supporting IT equipment disposal procedures, are developed, implemented and maintained.	Functional	Intersects With	Digital & Non-Digital Media Disposal	DCH-17	Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.	5		DCH-08			
ISM-1551	IT equipment management policy	An IT equipment management policy is developed, implemented and maintained.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10		GOV-02			
ISM-1552	Web application interactions	All web application content is offered exclusively using HTTPS.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-05	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5		TDA-06			
ISM-1552	Web application interactions	All web application content is offered exclusively using HTTPS.	Functional	Intersects With	Secure Web Traffic	WEB-09	Mechanisms exist to ensure all web application content is delivered using cryptographic mechanisms (e.g., TLS).	5		WEB-10			
ISM-1553	Configuring Transport Layer Security	TLS compression is disabled for TLS connections.	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03			
ISM-1554	Before travelling overseas with mobile devices	If travelling overseas with mobile devices to high or extreme risk countries, personnel are: • issued with newly provisioned user 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	Intersects With	Travel-Only Devices	AST-32	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		AST-24			
ISM-1555	Before travelling overseas with mobile devices	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 user accounts • backup all remaining data, applications and settings.	Functional	Intersects With	Travel-Only Devices	AST-32	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		AST-24			
ISM-1556	After travelling overseas with mobile devices	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 user accounts for any indicators of compromise, such as failed logon attempts.	Functional	Intersects With	Travel-Only Devices	AST-32	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		AST-24			
ISM-1556	After travelling overseas with mobile devices	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 user accounts for any indicators of compromise, such as failed logon attempts.	Functional	Intersects With	Re-Imaging Devices After Travel	AST-33	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		AST-25			
ISM-1557	Password strength	Passwords used for single-factor authentication on SECRET systems are a minimum of 17 characters.	Functional	Intersects With	Password-Based Authentication	IAC-15	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5		IAC-10.1			
ISM-1558	Password strength	Passwords using a sequence of words for single-factor authentication are not constructed using: • a list of categorised words • a real sentence in a natural language • song lyrics, movie or television show quotes, literature, or any other publicly available material • less than 4 random words for non-classified, OFFICIAL: Sensitive and PROTECTED systems; 5 random words for SECRET systems; or 6 random words for TOP SECRET systems.	Functional	Intersects With	Password-Based Authentication	IAC-15	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5		IAC-10.1			
ISM-1559	Password strength	Passwords used for multi-factor authentication on non-classified, OFFICIAL: Sensitive and PROTECTED systems are a minimum of 6 characters.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5		IAC-06			
ISM-1560	Password strength	Passwords used for multi-factor authentication on SECRET systems are a minimum of 8 characters.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5		IAC-06			
ISM-1561	Password strength	Passwords used for multi-factor authentication on TOP SECRET systems are a minimum of 10 characters.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5		IAC-06			
ISM-1562	Video conferencing and Internet Protocol telephony infrastructure hardening	Video conferencing and IP telephony infrastructure is hardened.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1562	Video conferencing and Internet Protocol telephony infrastructure hardening	Video conferencing and IP telephony infrastructure is hardened.	Functional	Intersects With	Video Teleconference (VTC) Security	CFG-04.16	Mechanisms exist to implement secure Video Teleconference (VTC) capabilities on endpoint devices and in designated conference rooms, to prevent potential eavesdropping.	5		AST-20			
ISM-1562	Video conferencing and Internet Protocol telephony infrastructure hardening	Video conferencing and IP telephony infrastructure is hardened.	Functional	Intersects With	Social Media & Social Networking Restrictions	HRS-06.2	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.	5		HRS-05.2			
ISM-1562	Video conferencing and Internet Protocol telephony infrastructure hardening	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		NET-03.2			
ISM-1563	Security assessment report	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	Intersects With	Security Assessment Report (SAR)	IAO-13	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.	5		IAO-02.4			
ISM-1564	Plan of action and milestones	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	Capabilities Deficiency Tracking	IAO-12	Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum: (1) Deficiency tracking number; (2) Applicable security, compliance and/or resilience control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection; (6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner); (8) Resources required to conduct remediation actions; (9) Planned remedial actions to the deficiency(ies); (10) Proposed remediation timeline; and (11) Disposition statement (e.g., closeout summary).	5		IAO-05			
ISM-1565	Providing cyber security awareness training	Tailored privileged user training is undertaken annually by all privileged users.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-05	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5		SAT-03			
ISM-1565	Providing cyber security awareness training	Tailored privileged user training is undertaken annually by all privileged users.	Functional	Intersects With	Privileged User Training	SAT-05.2	Mechanisms exist to provide specific training for privileged users to ensure privileged users understand their unique roles and responsibilities.	5		SAT-03.5			
ISM-1566	Unprivileged access to systems	Use of unprivileged access is centrally logged.	Functional	Intersects With	Centralized Collection of Event Logs & Security-Relevant Telemetry	MON-05	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of event logs and security-relevant telemetry.	5		MON-02			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-1567	Cyber supply chain risk management activities	Suppliers identified as high risk by a cyber supply chain risk assessment are not used.	Functional	Intersects With	Prohibited Technology Assets, Applications and/or Services (TAAS)	AST-12	Mechanisms exist to govern Supply Chain Risk Management (SCRM) sanctions that require the removal and prohibition of certain Technology Assets, Applications and/or Services (TAAS) that are designated as supply chain threats by: (1) A statutory or regulatory body; or (2) An internally performed risk assessment.	8	Updated 2026.3	AST-17			
ISM-1567	Cyber supply chain risk management activities	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-20	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology	5		RSK-09			
ISM-1567	Cyber supply chain risk management activities	Suppliers identified as high risk by a cyber supply chain risk assessment are not used.	Functional	Intersects With	Supply Chain Risk Assessment (SCRA)	RSK-21	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	5		RSK-09.1			
ISM-1567	Cyber supply chain risk management activities	Suppliers identified as high risk by a cyber supply chain risk assessment are not used.	Functional	Intersects With	Acquisition Strategies, Tools & Methods	TPM-03	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique Technology Assets, Applications	5		TPM-03.1			
ISM-1567	Cyber supply chain risk management activities	Suppliers identified as high risk by a cyber supply chain risk assessment are not used.	Functional	Intersects With	Limit Potential Harm	TPM-04.2	Mechanisms exist to utilize security safeguards to limit harm from potential adversaries who identify and target the organization's supply chain.	5		TPM-03.2			
ISM-1568	Cyber supply chain risk management activities	Operating systems, applications, IT equipment, OT equipment and services are procured from suppliers that have demonstrated a commitment to the security of their products and services.	Functional	Intersects With	Acquisition Strategies, Tools & Methods	TPM-03	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique Technology Assets, Applications and/or Services (TAAS).	5		TPM-03.1			
ISM-1568	Cyber supply chain risk management activities	Operating systems, applications, IT equipment, OT equipment and services are procured from suppliers that have demonstrated a commitment to the security of their products and services.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5		TPM-04.1			
ISM-1569	Cyber supply chain risk management activities	A shared responsibility model is created, documented and shared between suppliers and their customers to articulate the security responsibilities of each party.	Functional	Intersects With	Supply Chain Coordination	IRO-19	Mechanisms exist to provide cybersecurity and data protection incident information to the provider of the Technology Assets, Applications and/or Services (TAAS) and other organizations involved in the supply chain for TAAS related to the incident.	5		IRO-10.4			
ISM-1569	Cyber supply chain risk management activities	A shared responsibility model is created, documented and shared between suppliers and their customers to articulate the security responsibilities of each party.	Functional	Intersects With	Third-Party Services	TPM-12	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-04			
ISM-1569	Cyber supply chain risk management activities	A shared responsibility model is created, documented and shared between suppliers and their customers to articulate the security responsibilities of each party.	Functional	Intersects With	Third-Party Personnel Security	TPM-13	Mechanisms exist to control personnel security requirements including security roles and responsibilities for third-party providers.	5		TPM-06			
ISM-1569	Cyber supply chain risk management activities	A shared responsibility model is created, documented and shared between suppliers and their customers to articulate the security responsibilities of each party.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-05			
ISM-1570	Assessment of outsourced cloud service providers	Outsourced cloud service providers and their non-classified, OFFICIAL: Sensitive, PROTECTED and SECRET cloud services undergo an IRAP assessment, using the latest release of the ISM available prior to the beginning of the IRAP assessment (or a subsequent release), at least every 24 months.	Functional	Intersects With	Specialized Assessments	IAO-05	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 and OT); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; (11) Artificial Intelligence and Autonomous Technologies (AAT); and/or (12) Other Technology Assets, Applications and/or Services (TAAS) that require specialized expertise to determine conformity with security, compliance and/or resilience requirements.	5		IAO-02.2			
ISM-1571	Contractual security requirements with service providers	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-08	Mechanisms exist to protect sensitive and/or regulated data that is collected, developed, received, transmitted, used or stored in support of the performance of a contract.	5		IAO-03.2			
ISM-1571	Contractual security requirements with service providers	The right to verify compliance with security requirements is documented in contractual arrangements with service providers.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-05			
ISM-1572	Contractual security requirements with service providers	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	DCH-30.1	Mechanisms exist to control the location of Technology Assets, Applications and/or Services (TAAS) processing and/or storage based on business requirements that includes statutory, regulatory and contractual obligations.	5		CLD-09			
ISM-1572	Contractual security requirements with service providers	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-08	Mechanisms exist to protect sensitive and/or regulated data that is collected, developed, received, transmitted, used or stored in support of the performance of a contract.	5		IAO-03.2			
ISM-1572	Contractual security requirements with service providers	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-12.2	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	5		TPM-04.4			
ISM-1572	Contractual security requirements with service providers	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-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-05			
ISM-1573	Contractual security requirements with service providers	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-08	Mechanisms exist to protect sensitive and/or regulated data that is collected, developed, received, transmitted, used or stored in support of the performance of a contract.	5		IAO-03.2			
ISM-1573	Contractual security requirements with service providers	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-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5		TPM-04.1			
ISM-1573	Contractual security requirements with service providers	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-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-05			
ISM-1574	Contractual security requirements with service providers	The storage of data in a portable manner that enables 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-08	Mechanisms exist to protect sensitive and/or regulated data that is collected, developed, received, transmitted, used or stored in support of the performance of a contract.	5		IAO-03.2			
ISM-1574	Contractual security requirements with service providers	The storage of data in a portable manner that enables 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-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-05			
ISM-1575	Contractual security requirements with service providers	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-08	Mechanisms exist to protect sensitive and/or regulated data that is collected, developed, received, transmitted, used or stored in support of the performance of a contract.	5		IAO-03.2			
ISM-1575	Contractual security requirements with service providers	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-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-05			
ISM-1576	Access to systems by service providers	If an organisation's systems are accessed or administered by a service provider in an unauthorised manner, the organisation is immediately notified.	Functional	Intersects With	Security Compromise Notification Agreements	TPM-21.1	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 Technology Assets, Applications and/or Services (TAAS) that the organization utilizes.	5		TPM-05.1			
ISM-1577	Network segmentation and segregation	An organisation's networks are segregated from their service providers' networks.	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network resources.	5		NET-06			
ISM-1579	Capacity and availability planning and monitoring for online services	Cloud service providers' ability to scale resources dynamically in response to genuine spikes in demand is discussed and verified as part of capacity and availability planning for online services.	Functional	Subset Of	Capacity & Performance Management	CAP-02	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	10		CAP-01			
ISM-1579	Capacity and availability planning and monitoring for online services	Cloud service providers' ability to scale resources dynamically in response to genuine spikes 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		CAP-03			
ISM-1579	Capacity and availability planning and monitoring for online services	Cloud service providers' ability to scale resources dynamically in response to genuine spikes in demand is discussed and verified as part of capacity and availability planning for online services.	Functional	Intersects With	Resource Priority	CAP-04	Mechanisms exist to control resource utilization of Technology Assets, Applications and/or Services (TAAS) that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.	5		CAP-02			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Australia - Information Security Manual (ISM) (June 2026)
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-1579	Capacity and availability planning and monitoring for online services	Cloud service providers' ability to scale resources dynamically in response to genuine spikes in demand is discussed and verified as part of capacity and availability planning for online services.	Functional	Intersects With	Elastic Expansion	CAP-06	Mechanisms exist to automatically scale the resources available for Technology Assets, Applications and/or Services (TAAS), as demand conditions change.	5		CAP-05			
ISM-1579	Capacity and availability planning and monitoring for online services	Cloud service providers' ability to scale resources dynamically in response to genuine spikes in demand is discussed and verified as part of capacity and availability planning for online services.	Functional	Subset Of	Cloud Services	CLD-02	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	10		CLD-01			
ISM-1580	Capacity and availability planning and monitoring for online services	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-02	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	10		CAP-01			
ISM-1580	Capacity and availability planning and monitoring for online services	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		CAP-03			
ISM-1580	Capacity and availability planning and monitoring for online services	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-04	Mechanisms exist to control resource utilization of Technology Assets, Applications and/or Services (TAAS) that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.	5		CAP-02			
ISM-1580	Capacity and availability planning and monitoring for online services	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-02	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	10		CLD-01			
ISM-1581	Capacity and availability planning and monitoring for online services	Continuous real-time monitoring of the capacity and availability of online services is performed.	Functional	Subset Of	Capacity & Performance Management	CAP-02	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	10		CAP-01			
ISM-1581	Capacity and availability planning and monitoring for online services	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		CAP-03			
ISM-1581	Capacity and availability planning and monitoring for online services	Continuous real-time monitoring of the capacity and availability of online services is performed.	Functional	Intersects With	Resource Priority	CAP-04	Mechanisms exist to control resource utilization of Technology Assets, Applications and/or Services (TAAS) that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.	5		CAP-02			
ISM-1581	Capacity and availability planning and monitoring for online services	Continuous real-time monitoring of the capacity and availability of online services is performed.	Functional	Subset Of	Cloud Services	CLD-02	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	10		CLD-01			
ISM-1582	Application control	Application control rulesets are validated at least annually.	Functional	Intersects With	Baseline Configuration Reviews & Updates	CFG-07	Mechanisms exist to review and update secure baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and upgrades.	5	Updated 2026.3	CFG-02.1		ML2	ML3
ISM-1583	User identification	Personnel who are contractors are identified as such.	Functional	Intersects With	Identification & Authentication for Non-Organizational Users	IAC-33	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization.	5		IAC-03			
ISM-1584	Hardening operating system configurations	Unprivileged users are prevented from bypassing, disabling or modifying security functionality of operating systems.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1585	Web browsers	Web browser security settings cannot be changed by users.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5	Updated 2026.3	CFG-02			
ISM-1585	Web browsers	Web browser security settings cannot be changed by users.	Functional	Intersects With	Role-Based Permissions To Implement Changes	CHG-04.2	Mechanisms exist to limit the ability to implement Technology Asset, Application and/or Service (TAAS) changes to designated privileged roles.	5	Updated 2026.3	CHG-04.4			
ISM-1586	Monitoring data import and export	Data transfer logs are used to record all data imports and exports from systems.	Functional	Subset Of	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10		MON-01			
ISM-1586	Monitoring data import and export	Data transfer logs are used to record all data imports and exports from systems.	Functional	Intersects With	Analyze and Prioritize Monitoring Requirements	MON-03.2	Mechanisms exist to assess the organization's needs for monitoring and prioritize the monitoring of Technology Assets, Applications and/or Services (TAAS), based on TAAS criticality and the sensitivity of the data it stores, transmits and processes.	5		MON-01.16			
ISM-1587	Annual reporting of system security status	System owners report the security status of each system to its authorising officer at least annually.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	5		GOV-17			
ISM-1588	Standard Operating Environments	SOEs are reviewed and updated at least annually.	Functional	Intersects With	Baseline Configuration Reviews & Updates	CFG-07	Mechanisms exist to review and update secure baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and upgrades.	5		CFG-02.1			
ISM-1589	Email server transport encryption	MTA-STS is enabled to prevent the unencrypted transfer of emails between email servers.	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03			
ISM-1589	Email server transport encryption	MTA-STS is enabled to prevent the unencrypted transfer of emails between email servers.	Functional	Intersects With	Electronic Messaging	NET-40.1	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5		NET-13			
ISM-1590	Changing credentials	Credentials for user accounts 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 user account changes.	Functional	Intersects With	Protection of Authenticators	IAC-14.2	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	5		IAC-10.5			
ISM-1591	Suspension of access to systems	Access to systems and their resources are removed or suspended as soon as practicable when personnel are detected undertaking malicious activities.	Functional	Intersects With	Account Disabling for High Risk Individuals	IAC-08.5	Mechanisms exist to disable accounts immediately upon notification for users posing a significant risk to the organization.	5		IAC-15.6			
ISM-1591	Suspension of access to systems	Access to systems and their resources are removed or suspended as soon as practicable when personnel are detected undertaking malicious activities.	Functional	Intersects With	Expeditious Remote Access Disconnect / Disable Capability	NET-26.2	Mechanisms exist to provide the capability to expeditiously disconnect or disable a user's remote access session.	5		NET-14.8			
ISM-1592	Application management	Unprivileged users do not have the ability to install unapproved applications.	Functional	Intersects With	Restrict Roles Permitted To Install Software	CFG-12	Automated mechanisms exist to prevent the installation of software, unless the action is performed by a privileged user or service.	5	Updated 2026.3	CFG-05			
ISM-1592	Application management	Unprivileged users do not have the ability to install unapproved applications.	Functional	Intersects With	Prohibit Non-Privileged Users from Executing Privileged Functions	IAC-30.1	Mechanisms exist to prevent non-privileged users from executing privileged functions to include disabling, circumventing or altering implemented security safeguards / countermeasures.	5		IAC-21.5			
ISM-1593	Setting credentials for user accounts	Users provide sufficient evidence to verify their identity when requesting new credentials.	Functional	Intersects With	Authenticator Management	IAC-14	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.	5		IAC-10			
ISM-1594	Setting credentials for user accounts	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	Intersects With	Authenticator Management	IAC-14	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.	5		IAC-10			
ISM-1595	Setting credentials for user accounts	Credentials provided to users are changed on first use.	Functional	Intersects With	Authenticator Management	IAC-14	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.	5		IAC-10			
ISM-1596	Setting credentials for user accounts	Credentials are not reused by users across different systems.	Functional	Intersects With	Password-Based Authentication	IAC-15	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5		IAC-10.1			
ISM-1597	Protecting credentials	Credentials are obscured as they are entered into systems.	Functional	Intersects With	Protection of Authenticators	IAC-14.2	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	5		IAC-10.5			
ISM-1598	Inspection of IT equipment following maintenance or repairs	Following maintenance or repairs to IT equipment, it is inspected to confirm that it retains its approved configuration and that no unauthorised modifications have been made.	Functional	Intersects With	Maintenance Validation	MNT-07	Mechanisms exist to validate: (1) Maintenance activities were appropriately performed according to the work order; and (2) Applicable security, compliance and resilience controls are operational.	5		MNT-10			
ISM-1599	Handling IT equipment	IT equipment is handled in a manner suitable for its sensitivity or classification.	Functional	Subset Of	Data Protection	DCH-02	Mechanisms exist to facilitate the implementation of data protection controls.	10		DCH-01			
ISM-1599	Handling IT equipment	IT equipment is handled in a manner suitable for its sensitivity or classification.	Functional	Intersects With	Component Marking	PES-18	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		PES-16			
ISM-1600	Sanitising media before first use	Media is sanitised before it is used for the first time.	Functional	Intersects With	Digital Media Sanitization	DCH-18	Mechanisms exist to sanitize digital 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		DCH-09			
ISM-1600	Sanitising media before first use	Media is sanitised before it is used for the first time.	Functional	Intersects With	First Time Use Sanitization	DCH-18.4	Mechanisms exist to apply nondestructive sanitization techniques to portable storage devices prior to first use.	5		DCH-09.4			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-1601	Hardening operating system configurations	Microsoft's attack surface reduction rules are implemented.	Functional	Intersects With	Unsupported Internet Browsers & Email Clients	CFG-15	Mechanisms exist to allow only approved Internet browsers and email clients to run on systems.	5		CFG-04.2			
ISM-1602	Communication of cyber security documentation	Cyber security documentation, including notification of subsequent changes, is communicated to all stakeholders.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10		GOV-02			
ISM-1603	Insecure authentication methods	Authentication methods susceptible to replay attacks are disabled.	Functional	Intersects With	Replay-Resistant Authentication	IAC-03.1	Automated mechanisms exist to employ replay-resistant authentication.	5		IAC-02.2			
ISM-1603	Insecure authentication methods	Authentication methods susceptible to replay attacks are disabled.	Functional	Intersects With	Identification & Authentication for Devices	IAC-34	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		IAC-04			
ISM-1604	Functional separation between operating environments	When using a software-based isolation mechanism that consumes shared physical computing resources, 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	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1604	Functional separation between operating environments	When using a software-based isolation mechanism that consumes shared physical computing resources, 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-23	Mechanisms exist to utilize virtualization techniques to support the employment of a diversity of operating systems and applications.	5		SEA-13.1			
ISM-1605	Functional separation between operating environments	When using a software-based isolation mechanism that consumes shared physical computing resources, the underlying operating system is hardened.	Functional	Intersects With	Virtualization Techniques	SEA-23	Mechanisms exist to utilize virtualization techniques to support the employment of a diversity of operating systems and applications.	5		SEA-13.1			
ISM-1606	Functional separation between operating environments	When using a software-based isolation mechanism that consumes shared physical computing resources, patches, updates or vendor mitigations for vulnerabilities are applied to the isolation mechanism and underlying operating system in a timely manner.	Functional	Intersects With	Virtualization Techniques	SEA-23	Mechanisms exist to utilize virtualization techniques to support the employment of a diversity of operating systems and applications.	5		SEA-13.1			
ISM-1607	Functional separation between operating environments	When using a software-based isolation mechanism that consumes shared physical resources, integrity monitoring and centralised event logging is performed for the isolation mechanism and underlying operating system.	Functional	Intersects With	Virtualization Techniques	SEA-23	Mechanisms exist to utilize virtualization techniques to support the employment of a diversity of operating systems and applications.	5		SEA-13.1			
ISM-1608	Standard Operating Environments	SOEs provided by third parties are scanned for malicious code and configurations.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1608	Standard Operating Environments	SOEs provided by third parties are scanned for malicious code and configurations.	Functional	Intersects With	Malicious Code Protection (Antimalware)	END-04	Mechanisms exist to utilize antimalware, or similar technologies, to detect and eradicate malicious code.	5		END-04			
ISM-1608	Standard Operating Environments	SOEs provided by third parties are scanned for malicious code and configurations.	Functional	Intersects With	Heuristic / Nonsignature-Based Malware Detection	END-04.2	Mechanisms exist to utilize heuristic / nonsignature-based antimalware detection capabilities.	5		END-04.4			
ISM-1609	Handling and containing intrusions	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-02	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10		IRO-01			
ISM-1609	Handling and containing intrusions	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-13	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		IRO-08			
ISM-1609	Handling and containing intrusions	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-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5		IRO-10			
ISM-1609	Handling and containing intrusions	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-16.1	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	5		IRO-09			
ISM-1610	Emergency access to systems	A method of emergency access to systems and their resources is documented and tested at least once when initially implemented and each time fundamental information technology infrastructure changes occur.	Functional	Intersects With	Emergency Accounts	IAC-11	Mechanisms exist to establish and control "emergency access only" accounts.	5		IAC-15.9			
ISM-1611	Emergency access to systems	Break glass accounts are only used when normal authentication processes cannot be used.	Functional	Intersects With	Emergency Accounts	IAC-11	Mechanisms exist to establish and control "emergency access only" accounts.	5		IAC-15.9			
ISM-1612	Emergency access to systems	Break glass accounts are only used for specific authorised activities.	Functional	Intersects With	Emergency Accounts	IAC-11	Mechanisms exist to establish and control "emergency access only" accounts.	5		IAC-15.9			
ISM-1613	Emergency access to systems	Use of break glass accounts is centrally logged.	Functional	Intersects With	Emergency Accounts	IAC-11	Mechanisms exist to establish and control "emergency access only" accounts.	5		IAC-15.9			
ISM-1614	Emergency access to systems	Break glass account credentials are changed by the account custodian after they are accessed by any other party.	Functional	Intersects With	Emergency Accounts	IAC-11	Mechanisms exist to establish and control "emergency access only" accounts.	5		IAC-15.9			
ISM-1615	Emergency access to systems	Break glass accounts are tested after credentials are changed.	Functional	Intersects With	Emergency Accounts	IAC-11	Mechanisms exist to establish and control "emergency access only" accounts.	5		IAC-15.9			
ISM-1616	Vulnerability disclosure program	A vulnerability disclosure program is implemented to assist with the secure development and maintenance of products and services.	Functional	Intersects With	Vulnerability Disclosure Program (VDP)	THR-12	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of Technology Assets, Applications and/or Services (TAAS) that receives unsolicited input from the public about vulnerabilities in organizational TAAS.	5		THR-06			
ISM-1617	Overseeing the cyber security program	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	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-04.1	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5		GOV-03			
ISM-1618	Overseeing cyber security incident response activities	The CISO oversees their organisation's response to cyber security incidents.	Functional	Subset Of	Incident Response Operations	IRO-02	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10		IRO-01			
ISM-1618	Overseeing cyber security incident response activities	The CISO oversees their organisation's response to cyber security incidents.	Functional	Intersects With	Incident Handling	IRO-06	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		IRO-02			
ISM-1618	Overseeing cyber security incident response activities	The CISO oversees their organisation's response to cyber security incidents.	Functional	Intersects With	Integrated Security Incident Response Team (ISIRT)	IRO-11	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations.	5		IRO-07			
ISM-1619	Setting credentials for built-in Administrator accounts, break glass accounts, local administrator accounts and service accounts	Service accounts are created as group Managed Service Accounts.	Functional	Intersects With	Group Authentication	IAC-21.1	Mechanisms exist to require individuals to be authenticated with an individual authenticator when a group authenticator is utilized.	5		IAC-02.1			
ISM-1620	Microsoft Active Directory Domain Services security group memberships	Privileged user accounts are members of the Protected Users security group.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-10	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5		IAC-16			
ISM-1621	PowerShell	Windows PowerShell 2.0 is disabled or removed.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5	Updated 2026.3	CFG-02			
ISM-1622	PowerShell	PowerShell is configured to use Constrained Language Mode.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			ML3
ISM-1623	PowerShell	PowerShell module logging, script block logging and transcription events are centrally logged.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02		ML2	ML3
ISM-1624	PowerShell	PowerShell script block logs are protected by Protected Event Logging functionality.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1625	Insider threat mitigation program	An insider threat mitigation program is developed, implemented and maintained.	Functional	Intersects With	Insider Threats	MON-17.3	Mechanisms exist to monitor internal personnel activity for potential security incidents.	5		MON-16.1			
ISM-1625	Insider threat mitigation program	An insider threat mitigation program is developed, implemented and maintained.	Functional	Intersects With	Insider Threat Program	THR-15	Mechanisms exist to implement an insider threat program that includes a cross-discipline insider threat incident handling team.	5	Updated 2026.3	IRO-02.2			
ISM-1625	Insider threat mitigation program	An insider threat mitigation program is developed, implemented and maintained.	Functional	Intersects With	Insider Threat Awareness	THR-16	Mechanisms exist to utilize security awareness training on recognizing and reporting potential indicators of insider threat.	5		THR-05			
ISM-1626	Insider threat mitigation program	Legal advice is sought regarding the development and implementation of an insider threat mitigation program.	Functional	Intersects With	Insider Threat Program	THR-15	Mechanisms exist to implement an insider threat program that includes a cross-discipline insider threat incident handling team.	5	Updated 2026.3	IRO-02.2			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-1626	Insider threat mitigation program	Legal advice is sought regarding the development and implementation of an insider threat mitigation program.	Functional	Intersects With	Insider Threat Awareness	THR-16	Mechanisms exist to utilize security awareness training on recognizing and reporting potential indicators of insider threat.	5		THR-05			
ISM-1627	Blocking anonymity network traffic	Inbound network connections from anonymity networks are blocked.	Functional	Intersects With	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-31	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	5		NET-08			
ISM-1628	Blocking anonymity network traffic	Outbound network connections to anonymity networks are blocked.	Functional	Intersects With	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-31	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	5		NET-08			
ISM-1629	Using Diffie-Hellman	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-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		CRY-01			
ISM-1631	Cyber supply chain risk management activities	Suppliers of operating systems, applications, IT equipment, OT equipment and services associated with systems are identified.	Functional	Intersects With	Third-Party Inventories	TPM-08	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 Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-01.1			
ISM-1632	Cyber supply chain risk management activities	Operating systems, applications, IT equipment, OT equipment and services are procured from suppliers that have a strong track record of maintaining the security of their own systems.	Functional	Intersects With	Acquisition Strategies, Tools & Methods	TPM-03	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique Technology Assets, Applications and/or Services (TAAS).	5		TPM-03.1			
ISM-1632	Cyber supply chain risk management activities	Operating systems, applications, IT equipment, OT equipment and services are procured from suppliers that have a strong track record of maintaining the security of their own systems.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-04	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5		TPM-03			
ISM-1633	Protecting systems and their resources	System owners, in consultation with each system's authorising officer, determine the system boundary, business criticality, and security and resilience objectives for each system based on an assessment of the impact if it were to be compromised or attacked.	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-11	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for Technology Assets, Applications, Services and/or Data (TAASD) under their control.	5		GOV-15			
ISM-1634	Protecting systems and their resources	System owners, in consultation with each system's authorising officer, select controls for each system and tailor them to achieve desired security and resilience objectives.	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-11	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for Technology Assets, Applications, Services and/or Data (TAASD) under their control.	5		GOV-15			
ISM-1634	Protecting systems and their resources	System owners, in consultation with each system's authorising officer, select controls for each system and tailor them to achieve desired security and resilience objectives.	Functional	Intersects With	Select Controls	GOV-11.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for Technology Assets, Applications, Services and/or Data (TAASD) under their control.	5		GOV-15.1			
ISM-1635	Protecting systems and their resources	System owners implement controls for each system and its operating environment.	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-11	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for Technology Assets, Applications, Services and/or Data (TAASD) under their control.	5		GOV-15			
ISM-1635	Protecting systems and their resources	System owners implement controls for each system and its operating environment.	Functional	Intersects With	Implement Controls	GOV-11.2	Mechanisms exist to compel data and/or process owners to implement required security, compliance and resilience controls for Technology Assets, Applications, Services and/or Data (TAASD) under their control.	5		GOV-15.2			
ISM-1636	Protecting systems and their resources	System owners, in consultation with each system's authorising officer, ensure controls for each non-classified, OFFICIAL: Sensitive, PROTECTED and SECRET system and its operating environment undergo a security assessment by their organisation's own assessors or Infosec Registered Assessor Program (IRAP) assessors to determine if they have been implemented correctly and are operating as intended.	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-11	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for Technology Assets, Applications, Services and/or Data (TAASD) under their control.	5		GOV-15			
ISM-1636	Protecting systems and their resources	System owners, in consultation with each system's authorising officer, ensure controls for each non-classified, OFFICIAL: Sensitive, PROTECTED and SECRET system and its operating environment undergo a security assessment by their organisation's own assessors or Infosec Registered Assessor Program (IRAP) assessors to determine if they have been implemented correctly and are operating as intended.	Functional	Intersects With	Assess Controls	GOV-11.3	Mechanisms exist to compel data and/or process owners to assess if required security, compliance and resilience controls for Technology Assets, Applications, Services and/or Data (TAASD) under their control are: (1) Designed to meet control objectives; (2) Implemented correctly; and (3) Operating as intended.	5		GOV-15.3			
ISM-1637	Outsourced cloud services	An outsourced cloud service register is developed, implemented, maintained and regularly verified.	Functional	Intersects With	Third-Party Inventories	TPM-08	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 Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-01.1			
ISM-1638	Outsourced cloud services	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	Intersects With	Third-Party Inventories	TPM-08	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 Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-01.1			
ISM-1639	Labelling building management cables	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	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-1640	Labelling cables for foreign systems in Australian facilities	Cables for foreign systems installed in Australian facilities are labelled at inspection points.	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-1641	Degaussing magnetic media	Following the use of a degausser, magnetic media is physically damaged by deforming any internal platters.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	5		AST-09			
ISM-1642	Sanitising media before first use	Media is sanitised before it is reused in a different security domain.	Functional	Intersects With	First Time Use Sanitization	DCH-18.4	Mechanisms exist to apply nondestructive sanitization techniques to portable storage devices prior to first use.	5		DCH-09.4			
ISM-1643	Software registers	Software registers contain versions and patch histories of applications, drivers, operating systems and firmware.	Functional	Intersects With	Asset Inventories	AST-04	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5		AST-02			
ISM-1644	Using mobile devices in public spaces	Sensitive or classified phone calls and conversations are not conducted in public locations unless care is taken to reduce the chance of conversations being overheard.	Functional	Intersects With	Social Media & Social Networking Restrictions	HRS-06.2	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.	5		HRS-05.2			
ISM-1644	Using mobile devices in public spaces	Sensitive or classified phone calls and conversations 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-16	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		PES-12			
ISM-1645	Floor plan diagrams	Floor plan diagrams are developed, implemented, maintained and regularly verified.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-17	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 and/or regulated data flows.	5		AST-04			
ISM-1646	Floor plan diagrams	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	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-17	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 and/or regulated data flows.	5		AST-04			
ISM-1647	Suspension of access to systems	Privileged access to systems and their resources are disabled after 12 months unless revalidated.	Functional	Intersects With	Attribute-Based Access Control (ABAC)	IAC-07	Automated mechanisms exist to enforce Attribute-Based Access Control (ABAC) through policy-driven, dynamic authorizations to: (1) Enforce usage conditions for users and/or role; and (2) Support the secure sharing of information.	5	Updated 2026.3	IAC-29			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Australia - Information Security Manual (ISM) (June 2026)
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-1647	Suspension of access to systems	Privileged access to systems and their resources are disabled after 12 months unless revalidated.	Functional	Intersects With	Periodic Review of Individual & Service Account Privileges	IAC-12	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	Updated 2026.3	IAC-17			
ISM-1648	Suspension of access to systems	Privileged access to systems and their resources are disabled after 45 days of inactivity.	Functional	Intersects With	Attribute-Based Access Control (ABAC)	IAC-07	Automated mechanisms exist to enforce Attribute-Based Access Control (ABAC) through policy-driven, dynamic authorizations to: (1) Enforce usage conditions for users and/or role; and (2) Support the secure sharing of information.	5	Updated 2026.3	IAC-29			
ISM-1648	Suspension of access to systems	Privileged access to systems and their resources are disabled after 45 days of inactivity.	Functional	Intersects With	Disable Inactive Accounts	IAC-08.4	Automated mechanisms exist to disable inactive accounts after an organization-defined time period.	5	Updated 2026.3	IAC-15.3			
ISM-1648	Suspension of access to systems	Privileged access to systems and their resources are disabled after 45 days of inactivity.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-10	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5	Updated 2026.3	IAC-16			
ISM-1648	Suspension of access to systems	Privileged access to systems and their resources are disabled after 45 days of inactivity.	Functional	Intersects With	Periodic Review of Individual & Service Account Privileges	IAC-12	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	Updated 2026.3	IAC-17			
ISM-1649	Privileged access to systems	Just-in-time administration is used for the administration of systems and their resources.	Functional	Intersects With	Automated System Account Management (Directory Services)	IAC-08.1	Automated mechanisms exist to support the management of system accounts (e.g., directory services).	3	Updated 2026.3	IAC-15.1			ML3
ISM-1649	Privileged access to systems	Just-in-time administration is used for the administration of systems and their resources.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-10	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	8	Updated 2026.3	IAC-16			ML3
ISM-1650	Privileged access to systems	Privileged user account and security group management events are centrally logged.	Functional	Intersects With	Centralized Collection of Event Logs & Security-Relevant Telemetry	MON-05	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of event logs and security-relevant telemetry.	8	Updated 2026.3	MON-02		ML2	ML3
ISM-1650	Privileged access to systems	Privileged user account and security group management events are centrally logged.	Functional	Intersects With	Privileged Functions Logging	MON-14	Mechanisms exist to log and review the actions of users and/or services with elevated privileges.	8	Updated 2026.3	MON-03.3		ML2	ML3
ISM-1650	Privileged access to systems	Privileged user account and security group management events are centrally logged.	Functional	Intersects With	Account Creation and Modification Logging	MON-14.1	Automated mechanisms exist to generate event logs for permissions changes to privileged accounts and/or groups.	3	Updated 2026.3	MON-16.4		ML2	ML3
ISM-1654	Hardening operating system configurations	Internet Explorer 11 is disabled or removed.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02	ML1	ML2	ML3
ISM-1654	Hardening operating system configurations	Internet Explorer 11 is disabled or removed.	Functional	Intersects With	Unsupported Internet Browsers & Email Clients	CFG-15	Mechanisms exist to allow only approved Internet browsers and email clients to run on systems.	5		CFG-04.2	ML1	ML2	ML3
ISM-1655	Hardening operating system configurations	.NET Framework 3.5 (includes .NET 2.0 and 3.0) is disabled or removed.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5	Updated 2026.3	CFG-02			
ISM-1656	Application control	Application control is implemented on non-internet-facing servers.	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-05	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive secure baseline configurations.	5		CFG-02.5			ML3
ISM-1657	Application control	Application control restricts the execution of executables, libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5	Updated 2026.3	CFG-02	ML1	ML2	ML3
ISM-1658	Application control	Application control restricts the execution of drivers to an organisation-approved set.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5	Updated 2026.3	CFG-02			ML3
ISM-1659	Application control	Microsoft's vulnerable driver blocklist is implemented.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5	Updated 2026.3	CFG-02			ML3
ISM-1660	Application control	Allowed and blocked application control events are centrally logged.	Functional	Intersects With	Centralized Collection of Event Logs & Security-Relevant Telemetry	MON-05	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of event logs and security-relevant telemetry.	5	Updated 2026.3	MON-02		ML2	ML3
ISM-1660	Application control	Allowed and blocked application control events are centrally logged.	Functional	Intersects With	Content of Event Logs	MON-09	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5	Updated 2026.3	MON-03		ML2	ML3
ISM-1667	Office productivity suites	Microsoft Office is blocked from creating child processes.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5	Updated 2026.3	CFG-02		ML2	ML3
ISM-1668	Office productivity suites	Microsoft Office is blocked from creating executable content.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5	Updated 2026.3	CFG-02		ML2	ML3
ISM-1669	Office productivity suites	Microsoft Office is blocked from injecting code into other processes.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5	Updated 2026.3	CFG-02		ML2	ML3
ISM-1670	Portable Document Format applications	PDF applications are blocked from creating child processes.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5	Updated 2026.3	CFG-02		ML2	ML3
ISM-1671	Office productivity suites	Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5	Updated 2026.3	CFG-02	ML1	ML2	ML3
ISM-1672	Office productivity suites	Microsoft Office macro antivirus scanning is enabled.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5	Updated 2026.3	CFG-02	ML1	ML2	ML3
ISM-1673	Office productivity suites	Microsoft Office macros are blocked from making Win32 API calls.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5	Updated 2026.3	CFG-02		ML2	ML3
ISM-1674	Office productivity suites	Only Microsoft Office macros running from within a sandboxed environment, a Trusted Location or that are digitally signed by a trusted publisher are allowed to execute.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5	Updated 2026.3	CFG-02			ML3
ISM-1675	Office productivity suites	Microsoft Office macros digitally signed by an untrusted publisher cannot be enabled via the Message Bar or Backstage View.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5	Updated 2026.3	CFG-02			ML3
ISM-1676	Office productivity suites	Microsoft Office's list of trusted publishers is validated at least annually.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5	Updated 2026.3	CFG-02			ML3
ISM-1679	Multi-factor authentication	Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation's sensitive data.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5		IAC-06	ML1	ML2	ML3
ISM-1680	Multi-factor authentication	Multi-factor authentication (where available) is used to authenticate users to third-party online services that process, store or communicate their organisation's non-sensitive data.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5		IAC-06	ML1	ML2	ML3

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Australia - Information Security Manual (ISM) (June 2026)
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-1681	Multi-factor authentication	Multi-factor authentication is used to authenticate customers to online customer services that process, store or communicate sensitive customer data.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5		IAC-06	ML1	ML2	ML3
ISM-1682	Multi-factor authentication	Multi-factor authentication used for authenticating users of systems is phishing-resistant.	Functional	Equal	Phishing-Resistant Multi-Factor Authentication (MFA)	IAC-37.2	Automated mechanisms exist to enforce phishing-resistant Multi-Factor Authentication (MFA) through authenticators that are cryptographically bound to the verifier's identity, preventing credential relay by an impersonating party.	10	Updated 2026.3			ML2	ML3
ISM-1683	Multi-factor authentication	Successful and unsuccessful multi-factor authentication events are centrally logged.	Functional	Intersects With	Event Log & Security-Relevant Telemetry Monitoring	MON-03	Mechanisms exist to review event logs and security-relevant telemetry on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	8	Updated 2026.3	MON-01.8			
ISM-1683	Multi-factor authentication	Successful and unsuccessful multi-factor authentication events are centrally logged.	Functional	Intersects With	Centralized Collection of Event Logs & Security-Relevant Telemetry	MON-05	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of event logs and security-relevant telemetry.	8	Updated 2026.3	MON-02			
ISM-1685	Setting credentials for built-in Administrator accounts, break glass accounts, local administrator accounts and service accounts	Credentials for break glass accounts, local administrator accounts and service accounts are long, unique, unpredictable and managed.	Functional	Intersects With	Emergency Accounts	IAC-11	Mechanisms exist to establish and control "emergency access only" accounts.	5	Updated 2026.3	IAC-15.9		ML2	ML3
ISM-1686	Protecting credentials	Credential Guard functionality is enabled.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5	Updated 2026.3	CFG-02			
ISM-1686	Protecting credentials	Credential Guard functionality is enabled.	Functional	Intersects With	Protection of Authenticators	IAC-14.2	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	3	Updated 2026.3	IAC-10.5			
ISM-1687	Separate privileged operating environments	Privileged operating environments are not virtualised within unprivileged operating environments.	Functional	Equal	Privileged Environments	SEA-32	Mechanisms exist to prevent privileged operating environments from existing within unprivileged operating environments, including physical or virtual deployments of Technology Assets, Applications and/or Services (TAAS).	10	Updated 2026.3	SEA-22			
ISM-1688	Separate privileged operating environments	Unprivileged user accounts cannot logon to privileged operating environments.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-06	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5	Updated 2026.3	IAC-08			
ISM-1688	Separate privileged operating environments	Unprivileged user accounts cannot logon to privileged operating environments.	Functional	Intersects With	Automated System Account Management (Directory Services)	IAC-08.1	Automated mechanisms exist to support the management of system accounts (e.g., directory services).	5	Updated 2026.3	IAC-15.1			
ISM-1689	Separate privileged operating environments	Privileged user accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.	Functional	Intersects With	Non-Privileged Access for Non-Security Functions	IAC-30.3	Mechanisms exist to prohibit privileged users from using privileged accounts, while performing non-security functions.	5	Updated 2026.3	IAC-21.2	ML1	ML2	ML3
ISM-1690	Mitigating known vulnerabilities	Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		VPM-05	ML1	ML2	ML3
ISM-1691	Mitigating known vulnerabilities	Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF applications, and security products are applied within two weeks of release.	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		VPM-05	ML1	ML2	
ISM-1692	Mitigating known vulnerabilities	Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF applications, and security products are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		VPM-05			ML3
ISM-1693	Mitigating known vulnerabilities	Patches, updates or other vendor mitigations for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF applications, and security products are applied within one month of release.	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		VPM-05		ML2	ML3
ISM-1694	Mitigating known vulnerabilities	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		VPM-05	ML1	ML2	ML3
ISM-1695	Mitigating known vulnerabilities	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within one month of release.	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		VPM-05	ML1	ML2	
ISM-1696	Mitigating known vulnerabilities	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		VPM-05			ML3
ISM-1697	Mitigating known vulnerabilities	Patches, updates or other vendor mitigations for vulnerabilities in drivers are applied within one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		VPM-05			ML3
ISM-1698	Vulnerability scanning	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services.	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5		VPM-06	ML1	ML2	ML3
ISM-1699	Vulnerability scanning	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 applications, and security products.	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5		VPM-06	ML1	ML2	ML3
ISM-1700	Vulnerability scanning	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 applications, and security products.	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5		VPM-06		ML2	ML3
ISM-1701	Vulnerability scanning	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices.	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5		VPM-06	ML1	ML2	ML3
ISM-1702	Vulnerability scanning	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices.	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5		VPM-06	ML1	ML2	ML3
ISM-1703	Vulnerability scanning	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in drivers.	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5		VPM-06			ML3
ISM-1704	Cessation of support	Office productivity suites, web browsers and their extensions, email clients, PDF applications, Adobe Flash Player, and security products that are no longer supported by vendors are removed.	Functional	Intersects With	Unsupported Technology Assets, Applications and/or Services (TAAS)	AST-39	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs.	5		TDA-17	ML1	ML2	ML3
ISM-1705	Backup access	Privileged user accounts (excluding backup administrator accounts) cannot access backups belonging to other user accounts.	Functional	Intersects With	Data Backup Access	BCD-30	Mechanisms exist to restrict access to data backups to those privileged users with assigned roles for data backup and recovery operations.	5	Updated 2026.3	BCD-11.9		ML2	ML3
ISM-1705	Backup access	Privileged user accounts (excluding backup administrator accounts) cannot access backups belonging to other user accounts.	Functional	Intersects With	Data Backup Modification and/or Destruction	BCD-33	Mechanisms exist to restrict access to modify and/or delete data backups to only those privileged users with assigned data backup and recovery operations roles.	5	Updated 2026.3	BCD-11.10			
ISM-1706	Backup access	Privileged user accounts (excluding backup administrator accounts) cannot access their own backups.	Functional	Intersects With	Data Backup Access	BCD-30	Mechanisms exist to restrict access to data backups to those privileged users with assigned roles for data backup and recovery operations.	5	Updated 2026.3	BCD-11.9			ML3
ISM-1706	Backup access	Privileged user accounts (excluding backup administrator accounts) cannot access their own backups.	Functional	Intersects With	Data Backup Modification and/or Destruction	BCD-33	Mechanisms exist to restrict access to modify and/or delete data backups to only those privileged users with assigned data backup and recovery operations roles.	5	Updated 2026.3	BCD-11.10			
ISM-1707	Backup modification and deletion	Privileged user accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups.	Functional	Intersects With	Data Backup Access	BCD-30	Mechanisms exist to restrict access to data backups to those privileged users with assigned roles for data backup and recovery operations.	5	Updated 2026.3	BCD-11.9			
ISM-1707	Backup modification and deletion	Privileged user accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups.	Functional	Intersects With	Data Backup Modification and/or Destruction	BCD-33	Mechanisms exist to restrict access to modify and/or delete data backups to only those privileged users with assigned data backup and recovery operations roles.	5	Updated 2026.3	BCD-11.10		ML2	ML3
ISM-1708	Backup modification and deletion	Backup administrator accounts are prevented from modifying and deleting backups during their retention period.	Functional	Intersects With	Resilient Data Backup Architecture	BCD-23	Mechanisms exist to maintain a secure, immutable backup architecture.	5	Updated 2026.3				
ISM-1708	Backup modification and deletion	Backup administrator accounts are prevented from modifying and deleting backups during their retention period.	Functional	Intersects With	Data Backup Modification and/or	BCD-33	Mechanisms exist to restrict access to modify and/or delete data backups to only those privileged users with	5	Updated 2026.3	BCD-11.10			ML3
ISM-1710	Default settings	Settings for wireless access points are hardened.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1711	802.1X authentication	User identity confidentiality is used if available with EAP-TLS implementations.	Functional	Subset Of	Network Security Controls (NSC)	NET-02	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10		NET-01			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-1712	Fast Basic Service Set Transition	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-02	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10		NET-01			
ISM-1713	Removable media register	A removable media register is developed, implemented, maintained and regularly verified.	Functional	Intersects With	Removable Media Security	DCH-21	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	5		DCH-12			
ISM-1717	Vulnerability disclosure program	A 'security.txt' file is hosted for each of an organisation's internet-facing website domains to assist in the responsible disclosure of vulnerabilities in the organisation's products and services.	Functional	Intersects With	Vulnerability Disclosure Program (VDP)	THR-12	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of Technology Assets, Applications and/or Services (TAAS) that receives unsolicited input from the public about vulnerabilities in organizational TAAS.	5		THR-06			
ISM-1718	Cable colours	SECRET cables are coloured salmon pink.	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-1718	Cable colours	SECRET cables are coloured salmon pink.	Functional	Intersects With	Component Marking	PES-18	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		PES-16			
ISM-1719	Cable colours	TOP SECRET cables are coloured red.	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-1719	Cable colours	TOP SECRET cables are coloured red.	Functional	Intersects With	Component Marking	PES-18	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		PES-16			
ISM-1720	Wall outlet box colours	SECRET wall outlet boxes are coloured salmon pink.	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-1720	Wall outlet box colours	SECRET wall outlet boxes are coloured salmon pink.	Functional	Intersects With	Component Marking	PES-18	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		PES-16			
ISM-1721	Wall outlet box colours	TOP SECRET wall outlet boxes are coloured red.	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-1721	Wall outlet box colours	TOP SECRET wall outlet boxes are coloured red.	Functional	Intersects With	Component Marking	PES-18	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		PES-16			
ISM-1722	Media destruction methods	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-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	5		AST-09			
ISM-1722	Media destruction methods	Electrostatic memory devices are destroyed using a furnace/incinerator, hammer mill, disintegrator or grinder/sander.	Functional	Intersects With	Digital & Non-Digital Media Disposal	DCH-17	Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.	5		DCH-08			
ISM-1723	Media destruction methods	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-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	5		AST-09			
ISM-1723	Media destruction methods	Magnetic floppy disks are destroyed using a furnace/incinerator, hammer mill, disintegrator, degausser or by cutting.	Functional	Intersects With	Digital & Non-Digital Media Disposal	DCH-17	Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.	5		DCH-08			
ISM-1724	Media destruction methods	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-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	5		AST-09			
ISM-1724	Media destruction methods	Magnetic hard disks are destroyed using a furnace/incinerator, hammer mill, disintegrator, grinder/sander or degausser.	Functional	Intersects With	Digital & Non-Digital Media Disposal	DCH-17	Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.	5		DCH-08			
ISM-1725	Media destruction methods	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-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	5		AST-09			
ISM-1725	Media destruction methods	Magnetic tapes are destroyed using a furnace/incinerator, hammer mill, disintegrator, degausser or by cutting.	Functional	Intersects With	Digital & Non-Digital Media Disposal	DCH-17	Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.	5		DCH-08			
ISM-1726	Media destruction methods	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-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	5		AST-09			
ISM-1726	Media destruction methods	Optical disks are destroyed using a furnace/incinerator, hammer mill, disintegrator, grinder/sander or by cutting.	Functional	Intersects With	Digital & Non-Digital Media Disposal	DCH-17	Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.	5		DCH-08			
ISM-1727	Media destruction methods	Semiconductor memory is destroyed using a furnace/incinerator, hammer mill or disintegrator.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	5		AST-09			
ISM-1727	Media destruction methods	Semiconductor memory is destroyed using a furnace/incinerator, hammer mill or disintegrator.	Functional	Intersects With	Digital & Non-Digital Media Disposal	DCH-17	Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.	5		DCH-08			
ISM-1728	Treatment of media waste particles	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-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	5		AST-09			
ISM-1728	Treatment of media waste particles	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-18	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		PES-16			
ISM-1729	Treatment of media waste particles	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-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	5		AST-09			
ISM-1729	Treatment of media waste particles	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-18	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		PES-16			
ISM-1730	Software bill of materials	A software bill of materials is produced and made available to consumers of software.	Functional	Intersects With	Software Bill of Materials (SBOM)	TDA-21.4	Mechanisms exist to generate, or obtain, a Software Bill of Materials (SBOM) for Technology Assets, Applications and/or Services (TAAS) that lists software packages in use, including versions and applicable licenses.	5		TDA-04.2			
ISM-1731	Handling and containing intrusions	Planning and coordination of intrusion remediation activities are conducted on a separate system to that which has been compromised.	Functional	Intersects With	Chain of Custody & Forensics	IRO-13	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		IRO-08			
ISM-1732	Handling and containing intrusions	To the extent possible, all intrusion remediation activities are conducted in a coordinated manner during the same planned outage.	Functional	Intersects With	Chain of Custody & Forensics	IRO-13	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		IRO-08			
ISM-1735	Media that cannot be successfully sanitised	Media that cannot be successfully sanitised is destroyed prior to its disposal.	Functional	Intersects With	Digital Media Sanitization	DCH-18	Mechanisms exist to sanitize digital 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		DCH-09			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-1736	Managed services	A managed service register is developed, implemented, maintained and regularly verified.	Functional	Intersects With	Third-Party Inventories	TPM-08	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 Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-01.1			
ISM-1737	Managed services	A managed service register contains the following for each managed service: • managed service provider's name • managed service's name • purpose for using the managed service • sensitivity or classification of data involved • due date for the next security assessment of the managed service • contractual arrangements for the managed service • point of contact for users of the managed service • 24/7 contact details for the managed service provider.	Functional	Intersects With	Third-Party Inventories	TPM-08	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 Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-01.1			
ISM-1738	Contractual security requirements with service providers	The right to verify compliance with security requirements documented in contractual arrangements with service providers is regularly exercised.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-05			
ISM-1739	Approval of cyber security documentation	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 Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5		PRM-07			
ISM-1739	Approval of cyber security documentation	A system's security architecture is approved prior to the development of the system.	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-08	Mechanisms exist to assess security, compliance and resilience controls as part of Technology Assets, Applications and/or Services (TAAS) project development to determine whether controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting requirements.	5		PRM-04			
ISM-1739	Approval of cyber security documentation	A system's security architecture is approved prior to the development of the system.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-09	Mechanisms exist to proactively govern Technology Assets, Applications and/or Services (TAAS) by: (1) Defining technical security, compliance and resilience requirements; and (2) Performing a criticality analysis at predefined decision points in the Secure Development Life Cycle (SDLC).	5		PRM-05			
ISM-1739	Approval of cyber security documentation	A system's security architecture is approved prior to the development of the system.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-04	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	5		SEA-02			
ISM-1739	Approval of cyber security documentation	A system's security architecture is approved prior to the development of the system.	Functional	Subset Of	Secure Engineering Principles	SEA-05	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10		SEA-01			
ISM-1739	Approval of cyber security documentation	A system's security architecture is approved prior to the development of the system.	Functional	Intersects With	Defense-In-Depth (DiD) Architecture	SEA-06	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		SEA-03			
ISM-1740	Managing and reporting suspicious changes to banking details or payment requests	Personnel dealing with banking details and payment requests are advised of what business email compromise is and how to manage and report it.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-04	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5		SAT-02			
ISM-1740	Managing and reporting suspicious changes to banking details or payment requests	Personnel dealing with banking details and payment requests are advised of what business email compromise is and how to manage and report it.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-05	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5		SAT-03			
ISM-1740	Managing and reporting suspicious changes to banking details or payment requests	Personnel dealing with banking details and payment requests are advised of what business email compromise is and how to manage and report it.	Functional	Intersects With	Suspicious Communications & Anomalous System Behavior	SAT-06.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.	5		SAT-03.2			
ISM-1741	IT equipment destruction processes and procedures	IT equipment destruction processes, and supporting IT equipment destruction procedures, are developed, implemented and maintained.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	5		AST-09			
ISM-1742	Sanitising IT equipment	IT equipment that cannot be sanitised is destroyed.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	5		AST-09			
ISM-1743	Operating system selection	Vendors that have demonstrated a commitment to Secure by Design and Secure by Default principles and practices, including secure programming practices and either memory-safe programming languages or less preferably memory-safe programming practices, are used for operating systems.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-04	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	5		SEA-02			
ISM-1743	Operating system selection	Vendors that have demonstrated a commitment to Secure by Design and Secure by Default principles and practices, including secure programming practices and either memory-safe programming languages or less preferably memory-safe programming practices, are used for operating systems.	Functional	Subset Of	Secure Engineering Principles	SEA-05	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10		SEA-01			
ISM-1743	Operating system selection	Vendors that have demonstrated a commitment to Secure by Design and Secure by Default principles and practices, including secure programming practices and either memory-safe programming languages or less preferably memory-safe programming practices, are used for operating systems.	Functional	Intersects With	Acquisition Strategies, Tools & Methods	TPM-03	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique Technology Assets, Applications and/or Services (TAAS).	5		TPM-03.1			
ISM-1745	Hardening operating system configurations	Early Launch Antimalware, Secure Boot, Trusted Boot and Measured Boot functionality is enabled.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1746	Application control	When implementing application control using path rules, only approved users can change file system permissions for approved files and folders.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-06	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5		IAC-08			
ISM-1748	Email clients	Email client security settings cannot be changed by users.	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-05	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive secure baseline configurations.	5		CFG-02.5			
ISM-1749	Protecting credentials	Cached credentials are limited to one previous logon.	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-05	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive secure baseline configurations.	5		CFG-02.5			
ISM-1749	Protecting credentials	Cached credentials are limited to one previous logon.	Functional	Intersects With	Protection of Authenticators	IAC-14.2	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	5		IAC-10.5			
ISM-1749	Protecting credentials	Cached credentials are limited to one previous logon.	Functional	Intersects With	Expiration of Cached Authenticators	IAC-14.5	Automated mechanisms exist to prohibit the use of cached authenticators after an organization-defined time period.	5	Updated 2026.3	IAC-10.10			
ISM-1750	Administrative infrastructure	Administrative infrastructure for critical servers, high-value servers and regular servers is segregated from each other.	Functional	Intersects With	Cloud Infrastructure Security Subnet	CLD-06	Mechanisms exist to host security-specific technologies in a dedicated subnet.	5		CLD-03			
ISM-1750	Administrative infrastructure	Administrative infrastructure for critical servers, high-value servers and regular servers is segregated from each other.	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network resources.	5		NET-06			
ISM-1750	Administrative infrastructure	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		NET-06.1			
ISM-1751	Mitigating known vulnerabilities	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	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		VPM-05			
ISM-1752	Vulnerability scanning	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	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5		VPM-06			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-1753	Cessation of support	Internet-facing network devices that are no longer supported by vendors are replaced.	Functional	Intersects With	Unsupported Technology Assets, Applications and/or Services (TAAS)	AST-39	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs.	5		TDA-17			
ISM-1754	Reporting and resolving vulnerabilities	Vulnerabilities identified in software are resolved in a timely manner.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-17	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience 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 control testing and evaluation process; and (3) Document the results.	5		TDA-09			
ISM-1755	Vulnerability disclosure program	A vulnerability disclosure policy is developed, implemented and maintained.	Functional	Intersects With	Vulnerability Disclosure Program (VDP)	THR-12	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of Technology Assets, Applications and/or Services (TAAS) that receives unsolicited input from the public about vulnerabilities in organizational TAAS.	5		THR-06			
ISM-1756	Vulnerability disclosure program	Vulnerability disclosure processes, and supporting vulnerability disclosure procedures, are developed, implemented and maintained.	Functional	Intersects With	Vulnerability Disclosure Program (VDP)	THR-12	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of Technology Assets, Applications and/or Services (TAAS) that receives unsolicited input from the public about vulnerabilities in organizational TAAS.	5		THR-06			
ISM-1759	Using Diffie-Hellman	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-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		CRY-01			
ISM-1761	Using Elliptic Curve Diffie-Hellman	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-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		CRY-01			
ISM-1762	Using Elliptic Curve Diffie-Hellman	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-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		CRY-01			
ISM-1763	Using the Elliptic Curve Digital Signature Algorithm	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-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		CRY-01			
ISM-1764	Using the Elliptic Curve Digital Signature Algorithm	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-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		CRY-01			
ISM-1765	Using Rivest-Shamir-Adleman	When using RSA for digital signatures, and transporting encryption session keys (and similar keys), a modulus of at least 3072 bits is used, preferably 3072 bits.	Functional	Subset Of	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		CRY-01			
ISM-1766	Using Secure Hashing Algorithms	When using SHA-2 for hashing, an output size of at least 224 bits is used, preferably SHA-384 or SHA-512.	Functional	Subset Of	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		CRY-01			
ISM-1767	Using Secure Hashing Algorithms	When using SHA-2 for hashing, an output size of at least 256 bits is used, preferably SHA-384 or SHA-512.	Functional	Subset Of	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		CRY-01			
ISM-1768	Using Secure Hashing Algorithms	When using SHA-2 for hashing, an output size of at least 384 bits is used, preferably SHA-384 or SHA-512.	Functional	Subset Of	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		CRY-01			
ISM-1769	Using symmetric cryptographic algorithms	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-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		CRY-01			
ISM-1770	Using symmetric cryptographic algorithms	When using AES for encryption, AES-192 or AES-256 is used, preferably AES-256.	Functional	Subset Of	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		CRY-01			
ISM-1771	Encryption algorithms	AES is used for encrypting IPsec connections, preferably ENCR_AES_GCM_16.	Functional	Subset Of	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		CRY-01			
ISM-1772	Pseudorandom function	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-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		CRY-01			
ISM-1773	System administrators for gateways	System administrators for gateways that connect to Australian Government Access Only networks are Australian nationals or seconded foreign nationals.	Functional	Intersects With	Citizenship Requirements	HRS-05.2	Mechanisms exist to verify that individuals accessing a system processing, storing, or transmitting sensitive and/or regulated data meet applicable statutory, regulatory and/or contractual requirements for citizenship.	5		HRS-04.3			
ISM-1774	System administration of gateways	Gateways are managed via a secure path isolated from all connected networks.	Functional	Subset Of	Network Security Controls (NSC)	NET-02	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10		NET-01			
ISM-1778	Manual import of data	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-25	Mechanisms exist to secure ad-hoc exchanges of large digital files with internal or external parties.	5		DCH-17			
ISM-1778	Manual import of data	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-44	Automated mechanisms exist to enforce resource containment protections that remove or quarantine a resource's access to other resources.	5		NET-08.4			
ISM-1779	Manual export of data	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-25	Mechanisms exist to secure ad-hoc exchanges of large digital files with internal or external parties.	5		DCH-17			
ISM-1779	Manual export of data	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-44	Automated mechanisms exist to enforce resource containment protections that remove or quarantine a resource's access to other resources.	5		NET-08.4			
ISM-1780	Secure software development	SecDevOps practices are used for software development.	Functional	Intersects With	Continuing Professional Education (CPE) - DevOps Personnel	SAT-08	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		SAT-03.8			
ISM-1780	Secure software development	SecDevOps practices are used for software development.	Functional	Subset Of	Technology Development & Acquisition	TDA-02	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10		TDA-01			
ISM-1781	Network encryption	All data communicated over network infrastructure is encrypted using ASD-approved cryptography.	Functional	Intersects With	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5		CRY-01			
ISM-1781	Network encryption	All data communicated over network infrastructure is encrypted using ASD-approved cryptography.	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03			
ISM-1782	Protective Domain Name System Services	A protective DNS service is used to block access to known malicious domain names.	Functional	Intersects With	Heuristic / Nonsignature-Based Malware Detection	END-04.2	Mechanisms exist to utilize heuristic / nonsignature-based antimalware detection capabilities.	5		END-04.4			
ISM-1782	Protective Domain Name System Services	A protective DNS service is used to block access to known malicious domain names.	Functional	Intersects With	Domain Name Service (DNS) Resolution	NET-13	Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.	5		NET-10			
ISM-1783	Border Gateway Protocol routing security	Public IP addresses controlled by, or used by, an organisation are signed by valid ROA records.	Functional	Subset Of	Network Security Controls (NSC)	NET-02	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10		NET-01			
ISM-1784	Cyber security incident management policy	The cyber security incident management policy, including the associated cyber security incident response plan, is exercised at least annually.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10		GOV-02			
ISM-1784	Cyber security incident management policy	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-08	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5		IRO-04			
ISM-1785	Supplier relationship management	A supplier relationship management policy is developed, implemented and maintained.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10		GOV-02			
ISM-1785	Supplier relationship management	A supplier relationship management policy is developed, implemented and maintained.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-20	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5		RSK-09			
ISM-1785	Supplier relationship management	A supplier relationship management policy is developed, implemented and maintained.	Functional	Subset Of	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	10		TPM-01			
ISM-1786	Supplier relationship management	An approved supplier list is developed, implemented and maintained.	Functional	Intersects With	Third-Party Inventories	TPM-08	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 Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-01.1			
ISM-1787	Sourcing operating systems, applications, IT equipment, OT equipment and services	Operating systems, applications, IT equipment, OT equipment and services are sourced from approved suppliers.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5		TPM-04.1			
ISM-1788	Sourcing operating systems, applications, IT equipment, OT equipment and services	Multiple potential suppliers are identified for sourcing critical operating systems, applications, IT equipment, OT equipment and services.	Functional	Intersects With	Acquisition Strategies, Tools & Methods	TPM-03	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique Technology Assets, Applications and/or Services (TAAS).	5		TPM-03.1			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-1789	Sourcing operating systems, applications, IT equipment, OT equipment and services	Sufficient spares of critical IT equipment and OT equipment are sourced and kept in reserve.	Functional	Intersects With	Reserve Hardware	BCD-20	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		BCD-15			
ISM-1789	Sourcing operating systems, applications, IT equipment, OT equipment and services	Sufficient spares of critical IT equipment and OT equipment are sourced and kept in reserve.	Functional	Intersects With	Acquisition Strategies, Tools & Methods	TPM-03	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique Technology Assets, Applications and/or Services (TAAS).	5		TPM-03.1			
ISM-1789	Sourcing operating systems, applications, IT equipment, OT equipment and services	Sufficient spares of critical IT equipment and OT equipment are sourced and kept in reserve.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-04	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5		TPM-03			
ISM-1790	Delivery of operating systems, applications, IT equipment, OT equipment and services	Operating systems, applications, IT equipment, OT equipment and services are delivered in a manner that maintains their integrity.	Functional	Intersects With	Provenance	AST-14	Mechanisms exist to track the origin, development, ownership, location and changes to Technology Assets, Applications, Services and/or Data (TAASD).	5		AST-03.2			
ISM-1790	Delivery of operating systems, applications, IT equipment, OT equipment and services	Operating systems, 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-09	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		TDA-11			
ISM-1791	Delivery of operating systems, applications, IT equipment, OT equipment and services	The integrity of operating systems, applications, IT equipment, OT equipment and services are assessed as part of acceptance of products and services.	Functional	Intersects With	Provenance	AST-14	Mechanisms exist to track the origin, development, ownership, location and changes to Technology Assets, Applications, Services and/or Data (TAASD).	5		AST-03.2			
ISM-1791	Delivery of operating systems, applications, IT equipment, OT equipment and services	The integrity of operating systems, 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-09	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		TDA-11			
ISM-1792	Delivery of operating systems, applications, IT equipment, OT equipment and services	The authenticity of operating systems, applications, IT equipment, OT equipment and services are assessed as part of acceptance of products and services.	Functional	Intersects With	Provenance	AST-14	Mechanisms exist to track the origin, development, ownership, location and changes to Technology Assets, Applications, Services and/or Data (TAASD).	5		AST-03.2			
ISM-1792	Delivery of operating systems, applications, IT equipment, OT equipment and services	The authenticity of operating systems, 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-09	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		TDA-11			
ISM-1793	Assessment of managed service providers	Managed service providers and their non-classified, OFFICIAL: Sensitive, PROTECTED and SECRET managed services undergo an Infosec Registered Assessor Program (IRAP) assessment, using the latest release of the ISM available prior to the beginning of the IRAP assessment (or a subsequent release), at least every 24 months.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08			
ISM-1793	Assessment of managed service providers	Managed service providers and their non-classified, OFFICIAL: Sensitive, PROTECTED and SECRET managed services undergo an Infosec Registered Assessor Program (IRAP) assessment, using the latest release of the ISM available prior to the beginning of the IRAP assessment (or a subsequent release), at least every 24 months.	Functional	Intersects With	Third-Party Scope Review	TPM-16	Mechanisms exist to perform recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure security, compliance and resilience control assignments accurately reflect current: (1) Contractual obligations for the External Service Provider (ESP); (2) Business practices; (3) Applicable stakeholders; and (4) Deployed Technology Assets, Applications and/or Services (TAAS).	5		TPM-05.5			
ISM-1794	Contractual security requirements with service providers	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	Intersects With	Managing Changes To Third-Party Services	TPM-17	Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.	5		TPM-10			
ISM-1795	Setting credentials for built-in Administrator accounts, break glass accounts, local administrator accounts and service accounts	Credentials for built-in Administrator accounts, break glass accounts, local administrator accounts and service accounts are a minimum of 30 characters.	Functional	Intersects With	Password-Based Authentication	IAC-15	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5		IAC-10.1			
ISM-1796	Secure software development	Files containing executable content are digitally signed by a certificate with a verifiable chain of trust as part of software development.	Functional	Intersects With	Signed Components	CHG-13	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		CHG-04.2			
ISM-1796	Secure software development	Files containing executable content are digitally signed by a certificate with a verifiable chain of trust as part of software development.	Functional	Intersects With	Product Management	TDA-06	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) 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		TDA-01.1			
ISM-1797	Secure software development	Installers, patches and updates are digitally signed or provided with cryptographic checksums as part of software development.	Functional	Intersects With	Product Management	TDA-06	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) 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		TDA-01.1			
ISM-1798	Secure software development	Secure configuration guidance, in the form of a hardening guide or loosening guide, is produced and made available to consumers as part of software development.	Functional	Intersects With	Product Management	TDA-06	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) 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		TDA-01.1			
ISM-1798	Secure software development	Secure configuration guidance, in the form of a hardening guide or loosening guide, is produced and made available to consumers as part of software development.	Functional	Intersects With	Functional Properties	TDA-08.2	Mechanisms exist to require software developers to provide information describing the functional properties of the security, compliance and resilience controls to be utilized within Technology Assets, Applications and/or Services (TAAS) in sufficient detail to permit analysis and testing of the controls.	5		TDA-04.1			
ISM-1798	Secure software development	Secure configuration guidance, in the form of a hardening guide or loosening guide, is produced and made available to consumers as part of software development.	Functional	Intersects With	Administrator Documentation	TDA-08.3	Mechanisms exist to obtain, protect and distribute administrator documentation for Technology Assets, Applications and/or Services (TAAS) that describe: (1) Secure configuration, installation and operation of the TAAS; (2) Effective use and maintenance of security features/functions; and (3) Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	5		TDA-04			
ISM-1798	Secure software development	Secure configuration guidance, in the form of a hardening guide or loosening guide, is produced and made available to consumers as part of software development.	Functional	Intersects With	Pre-Established Secure Configurations	TDA-13.1	Mechanisms exist to ensure vendors / manufacturers: (1) Deliver the Technology Asset, Application and/or Service (TAAS) with a pre-established, secure configuration implemented; and (2) Use the pre-established, secure configuration as the default for any subsequent TAAS reinstallation or upgrade.	5		TDA-02.4			
ISM-1799	Domain-based Message Authentication, Reporting and Conformance	Incoming emails are rejected if they do not pass DMARC checks.	Functional	Intersects With	Domain Name Service (DNS) Resolution	NET-13	Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.	5		NET-10			
ISM-1799	Domain-based Message Authentication, Reporting and Conformance	Incoming emails are rejected if they do not pass DMARC checks.	Functional	Intersects With	Sender Policy Framework (SPF)	NET-39.2	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		NET-10.3			
ISM-1800	Flashing network devices with trusted firmware before first use	Network devices are flashed with trusted firmware before they are used for the first time.	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-05	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive secure baseline configurations.	5		CFG-02.5			
ISM-1801	Regularly restarting network devices	Network devices are restarted at least monthly.	Functional	Intersects With	Continuous Vulnerability Remediation Activities	VPM-06.2	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	5		VPM-04			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-1802	High Assurance Cryptographic Equipment	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	Intersects With	Sensitive / Regulated Data Protection	DCH-07	Mechanisms exist to protect sensitive and/or regulated data wherever it is processed and/or stored.	5		DCH-01.2			
ISM-1803	Cyber security incident register	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-06	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		IRO-02			
ISM-1803	Cyber security incident register	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-16.1	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	5		IRO-09			
ISM-1804	Contractual security requirements with service providers	Break clauses associated with failure to meet security requirements are documented in contractual arrangements with service providers.	Functional	Intersects With	Break Clauses	TPM-19	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for security, compliance and/or resilience controls.	5		TPM-05.7			
ISM-1805	Denial of service response plan	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	Intersects With	Denial of Service (DoS) Protection	NET-21	Automated mechanisms exist to protect against or limit the effects of denial of service attacks.	5		NET-02.1			
ISM-1806	Hardening user application configurations	Default user accounts or credentials for user applications, including for any pre-configured user accounts, are changed, disabled or removed during initial setup.	Functional	Intersects With	Default Authenticators	IAC-14.4	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	5		IAC-10.8			
ISM-1807	Vulnerability scanning	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.	Functional	Intersects With	Asset Inventories	AST-04	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5		AST-02	ML1	ML2	ML3
ISM-1807	Vulnerability scanning	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-07	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	Updated 2026.3		ML1	ML2	ML3
ISM-1807	Vulnerability scanning	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.	Functional	Intersects With	Asset Discovery	AST-09	Automated mechanisms exist to perform asset discovery to identify Technology Assets, Applications and/or Services (TAAS) connected to organizational networks, including assets not present in existing inventories.	8	Updated 2026.3				
ISM-1808	Vulnerability scanning	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	Updated 2026.3	VPM-06			
ISM-1808	Vulnerability scanning	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	Functional	Intersects With	Update Vulnerability Scanning Tools	VPM-12.1	Mechanisms exist to update vulnerability scanning tools.	5	Updated 2026.3	VPM-06.1			
ISM-1809	Cessation of support	When applications, operating systems, network devices or networked 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	Intersects With	Compensating Countermeasures	RSK-18	Mechanisms exist to identify and implement one, or more, compensating controls to reduce risk and threat exposure when the primary means of implementing the security function is unavailable or compromised.	5		RSK-06.2			
ISM-1810	Performing and retaining backups	Backups of data, applications and settings are synchronised to enable restoration to a common point in time.	Functional	Intersects With	Synchronization With Authoritative Time Source	MON-11.1	Mechanisms exist to synchronize internal system clocks with an authoritative time source.	5	Updated 2026.3	MON-07.1			
ISM-1811	Performing and retaining backups	Backups of data, applications and settings are retained in a secure and resilient manner.	Functional	Intersects With	Resilient Data Backup Architecture	BCD-23	Mechanisms exist to maintain a secure, immutable backup architecture.	5	Updated 2026.3				
ISM-1811	Performing and retaining backups	Backups of data, applications and settings are retained in a secure and resilient manner.	Functional	Intersects With	Data Backups	BCD-24	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and	5		BCD-11	ML1	ML2	ML3
ISM-1811	Performing and retaining backups	Backups of data, applications and settings are retained in a secure and resilient manner.	Functional	Intersects With	Separate Storage for Critical Information	BCD-24.2	Mechanisms exist to store backup copies of critical software and other security-related information in a	3	Updated 2026.3	BCD-11.2	ML1	ML2	ML3
ISM-1812	Backup access	Unprivileged user accounts cannot access backups belonging to other user accounts.	Functional	Intersects With	Data Backup Access	BCD-30	Mechanisms exist to restrict access to data backups to those privileged users with assigned roles for data backup and recovery operations.	5		BCD-11.9	ML1	ML2	ML3
ISM-1813	Backup access	Unprivileged user accounts cannot access their own backups.	Functional	Intersects With	Data Backup Access	BCD-30	Mechanisms exist to restrict access to data backups to those privileged users with assigned roles for data backup and recovery operations.	5		BCD-11.9			ML3
ISM-1813	Backup access	Unprivileged user accounts cannot access their own backups.	Functional	Intersects With	Data Backup Modification and/or Destruction	BCD-33	Mechanisms exist to restrict access to modify and/or delete data backups to only those privileged users with assigned data backup and recovery operations roles.	5	Updated 2026.3	BCD-11.10			
ISM-1814	Backup modification and deletion	Unprivileged user accounts are prevented from modifying and deleting backups.	Functional	Intersects With	Data Backup Modification and/or Destruction	BCD-33	Mechanisms exist to restrict access to modify and/or delete data backups to only those privileged users with assigned data backup and recovery operations roles.	5	Updated 2026.3	BCD-11.10			
ISM-1815	Centralised event logging facility	Event logs are protected from unauthorised modification and deletion.	Functional	Intersects With	Protection of Event Logs & Security-Relevant Telemetry	MON-12	Mechanisms exist to protect event logs, security-relevant telemetry and audit tools from unauthorized access, modification and deletion.	8	Updated 2026.3	MON-08		ML2	ML3
ISM-1816	Authoritative source for software	Unauthorised modification of the authoritative source for software is prevented.	Functional	Intersects With	Provenance	AST-14	Mechanisms exist to track the origin, development, ownership, location and changes to Technology Assets, Applications, Services and/or Data (TAASD).	5		AST-03.2			
ISM-1817	Network application programming interfaces	Authentication and authorisation of clients is performed when clients call network APIs that facilitate access to data not authorised for release into the public domain and are accessible over the internet.	Functional	No Relationship	N/A	N/A	N/A	0					
ISM-1818	Network application programming interfaces	Authentication and authorisation of clients is performed when clients call network APIs that facilitate modification of data and are accessible over the internet.	Functional	No Relationship	N/A	N/A	N/A	0					
ISM-1819	Enacting cyber security incident response plans	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.	Functional	Subset Of	Incident Handling	IRO-06	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report	10	Updated 2026.3	IRO-02			
ISM-1819	Enacting cyber security incident response plans	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.	Functional	Subset Of	Incident Response Plan (IRP)	IRO-08	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	Updated 2026.3	IRO-04			
ISM-1820	Cable colours	Cables for individual systems use a consistent colour.	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-1821	Common cable bundles and conduits	TOP SECRET cables, when bundled together or run in conduit, are run exclusively in their own individual cable bundle or conduit.	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-1822	Wall outlet box colours	Wall outlet boxes for individual systems use a consistent colour.	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1			
ISM-1823	Office productivity suites	Office productivity suite security settings cannot be changed by users.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02		ML2	ML3
ISM-1823	Office productivity suites	Office productivity suite security settings cannot be changed by users.	Functional	Intersects With	Access Restriction For Change	CHG-04.1	Mechanisms exist to define, document, approve and enforce access restrictions associated with changes to Technology Assets, Applications and/or Services (TAAS).	5	Updated 2026.3	CHG-04		ML2	ML3
ISM-1824	Portable Document Format applications	PDF application security settings cannot be changed by users.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02		ML2	ML3

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-1825	Security products	Security product security settings cannot be changed by users.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1826	Server application selection	Vendors that have demonstrated a commitment to Secure by Design and Secure by Default principles and practices, including secure programming practices and either memory-safe programming languages or less preferably memory-safe programming practices, are used for server applications.	Functional	No Relationship	N/A	N/A	N/A	0					
ISM-1827	Microsoft Active Directory Domain Services domain controllers	Microsoft AD DS domain controllers are administered using dedicated domain administrator user accounts that are not used to administer other systems.	Functional	Intersects With	Dedicated Privileged Account	IAC-10.3	Mechanisms exist to assign dedicated privileged user accounts to be used solely for duties requiring privileged access.	5		IAC-16.4			
ISM-1828	Microsoft Active Directory Domain Services domain controllers	The Print Spooler service is disabled on Microsoft AD DS domain controllers.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1829	Microsoft Active Directory Domain Services domain controllers	Passwords are not stored in Group Policy Preferences.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1830	Microsoft Active Directory services	Security-relevant events for Microsoft AD DS domain controllers, Microsoft AD CS CA servers, Microsoft AD FS servers and Microsoft Entra Connect servers are centrally logged.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1832	Microsoft Active Directory Domain Services account hardening	Only service accounts and computer accounts are configured with Service Principal Names (SPNs).	Functional	Intersects With	Account Management	IAC-08	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and (3) Proactively govern individual, group, system, service, application, guest and temporary accounts.	3		IAC-15			
ISM-1833	Microsoft Active Directory Domain Services account hardening	User accounts are provisioned with the minimum privileges required.	Functional	Intersects With	Least Privilege	IAC-30	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		IAC-21			
ISM-1834	Microsoft Active Directory Domain Services account hardening	Duplicate SPNs do not exist within the domain.	Functional	Intersects With	Account Management	IAC-08	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and (3) Proactively govern individual, group, system, service, application, guest and temporary accounts.	5		IAC-15			
ISM-1835	Microsoft Active Directory Domain Services account hardening	Privileged user accounts are configured as sensitive and cannot be delegated.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-10	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5		IAC-16			
ISM-1836	Microsoft Active Directory Domain Services account hardening	User accounts require Kerberos pre-authentication.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1838	Microsoft Active Directory Domain Services account hardening	The UserPassword attribute for user accounts is not used.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1839	Microsoft Active Directory Domain Services account hardening	Account properties accessible by unprivileged users are not used to store passwords.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1840	Microsoft Active Directory Domain Services account hardening	User account passwords do not use reversible encryption.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1841	Microsoft Active Directory Domain Services account hardening	Unprivileged user accounts cannot add machines to the domain.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1842	Microsoft Active Directory Domain Services account hardening	Dedicated privileged service accounts are used to add machines to the domain.	Functional	Intersects With	Dedicated Privileged Account	IAC-10.3	Mechanisms exist to assign dedicated privileged user accounts to be used solely for duties requiring privileged access.	5		IAC-16.4			
ISM-1843	Microsoft Active Directory Domain Services account hardening	User accounts with unconstrained delegation are reviewed at least annually, and those without an SPN or demonstrated business requirement are removed.	Functional	No Relationship	N/A	N/A	N/A	0					
ISM-1844	Microsoft Active Directory Domain Services account hardening	Computer accounts that are not Microsoft AD DS domain controllers are not trusted for delegation to services.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1845	Microsoft Active Directory Domain Services security group memberships	When a user account is disabled, it is removed from all security group memberships.	Functional	Intersects With	Account Management	IAC-08	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and (3) Proactively govern individual, group, system, service, application, guest and temporary accounts.	5		IAC-15			
ISM-1846	Microsoft Active Directory Domain Services security group memberships	The Pre-Windows 2000 Compatible Access security group does not contain user accounts.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1847	Changing credentials	Credentials for the Kerberos Key Distribution Center's service account (KRBTGT) are changed twice, allowing for replication to all Microsoft AD DS domain controllers in-between each change, if the domain has been directly compromised, the domain is suspected of being compromised or they have not been changed in the past 12 months.	Functional	No Relationship	N/A	N/A	N/A	0					
ISM-1848	Functional separation between operating environments	When using a software-based isolation mechanism that consumes shared physical computing resources, the isolation mechanism or underlying operating system is replaced when it is no longer supported by a vendor.	Functional	Intersects With	Unsupported Technology Assets, Applications and/or Services (TAAS)	AST-39	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs.	5		TDA-17			
ISM-1849	Secure web application design and development	The OWASP Top 10 Proactive Controls are used in the development of web applications.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-05	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5		TDA-06			
ISM-1850	Secure web application design and development	The OWASP Top 10 are mitigated in the development of web applications.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-17	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience 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 control testing and evaluation process; and (3) Document the results.	5		TDA-09			
ISM-1851	Web application programming interfaces	The OWASP API Security Top 10 are mitigated in the development of web APIs.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-17	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience 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 control testing and evaluation process; and (3) Document the results.	5		TDA-09			
ISM-1852	Unprivileged access to systems	Unprivileged access to systems and their resources is limited to only what is required for users and services to undertake their duties.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-06	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5		IAC-08			
ISM-1854	Authenticating to multifunction devices	Users authenticate to MFDs before they can print, scan or copy documents.	Functional	Intersects With	Multi-Function Devices (MFD)	CFG-04.12	Mechanisms exist to securely configure Multi-Function Devices (MFD) according to industry-recognized secure practices for the type of device.	5		AST-23			
ISM-1855	Logging multifunction device use	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)	CFG-04.12	Mechanisms exist to securely configure Multi-Function Devices (MFD) according to industry-recognized secure practices for the type of device.	5		AST-23			
ISM-1858	Hardening IT equipment configurations	IT equipment is hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-1859	Office productivity suites	Office productivity suites are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02		ML2	ML3
ISM-1860	Portable Document Format applications	PDF applications are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02		ML2	ML3
ISM-1861	Protecting credentials	Local Security Authority protection functionality is enabled.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			ML3
ISM-1862	Using web application firewalls	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	Intersects With	Web Application Firewall (WAF)	NET-34	Mechanisms exist to deploy Web Application Firewalls (WAFs) to provide defense-in-depth protection for application-specific threats.	5		WEB-03			
ISM-1863	Networked management interfaces	Networked management interfaces for IT equipment are not directly exposed to the internet.	Functional	Intersects With	Direct Internet Access Restrictions	NET-03.4	Mechanisms exist to prohibit, or strictly-control, Internet access from sensitive and/or regulated data enclaves (secure zones).	5		NET-06.5			
ISM-1864	System usage policy	A system usage policy is developed, implemented and maintained.	Functional	Subset Of	Rules of Behavior	HRS-06.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	10		HRS-05.1			
ISM-1865	System access requirements	Personnel agree to abide by system usage policies before being granted access to systems and their resources.	Functional	Intersects With	Terms of Employment	HRS-06	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to enable secure, compliant and resilient capabilities.	5		HRS-05			
ISM-1866	Privately owned mobile devices and desktop computers	Personnel using privately owned mobile devices or desktop computers to access OFFICIAL: Sensitive or PROTECTED systems or data are prevented from storing classified data on their privately owned mobile devices and desktop computers.	Functional	Intersects With	Technology Use Restrictions	HRS-06.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	5		HRS-05.3			
ISM-1866	Privately owned mobile devices and desktop computers	Personnel using privately owned mobile devices or desktop computers to access OFFICIAL: Sensitive or PROTECTED systems or data are prevented from storing classified data on their privately owned mobile devices and desktop computers.	Functional	Intersects With	Use of Mobile Devices	HRS-06.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5		HRS-05.5			
ISM-1867	Approved mobile platforms	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	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-05	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive secure baseline configurations.	5		CFG-02.5			
ISM-1868	Encrypted storage	SECRET and TOP SECRET mobile devices do not use removable media unless approved beforehand by ASD.	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-05	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive secure baseline configurations.	5		CFG-02.5			
ISM-1869	IT equipment registers	A non-networked IT equipment register is developed, implemented, maintained and regularly verified.	Functional	No Relationship	N/A	N/A	N/A	0					
ISM-1870	Application control	Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02	ML1	ML2	ML3
ISM-1871	Application control	Application control is applied to all locations other than user profiles and temporary folders used by operating systems, web browsers and email clients.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02		ML2	ML3
ISM-1872	Multi-factor authentication	Multi-factor authentication used for authenticating users of online services is phishing-resistant.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5		IAC-06		ML2	ML3
ISM-1872	Multi-factor authentication	Multi-factor authentication used for authenticating users of online services is phishing-resistant.	Functional	Intersects With	Phishing-Resistant Multi-Factor Authentication (MFA)	IAC-37.2	Automated mechanisms exist to enforce phishing-resistant Multi-Factor Authentication (MFA) through authenticators that are cryptographically bound to the verifier's identity, preventing credential relay by an impersonating party.	8	Updated 2026.3				
ISM-1873	Multi-factor authentication	Multi-factor authentication used for authenticating customers of online customer services provides a phishing-resistant option.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5		IAC-06		ML2	
ISM-1873	Multi-factor authentication	Multi-factor authentication used for authenticating customers of online customer services provides a phishing-resistant option.	Functional	Intersects With	Phishing-Resistant Multi-Factor Authentication (MFA)	IAC-37.2	Automated mechanisms exist to enforce phishing-resistant Multi-Factor Authentication (MFA) through authenticators that are cryptographically bound to the verifier's identity, preventing credential relay by an impersonating party.	8	Updated 2026.3				
ISM-1874	Multi-factor authentication	Multi-factor authentication used for authenticating customers of online customer services is phishing-resistant.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5		IAC-06			ML3
ISM-1874	Multi-factor authentication	Multi-factor authentication used for authenticating customers of online customer services is phishing-resistant.	Functional	Intersects With	Phishing-Resistant Multi-Factor Authentication (MFA)	IAC-37.2	Automated mechanisms exist to enforce phishing-resistant Multi-Factor Authentication (MFA) through authenticators that are cryptographically bound to the verifier's identity, preventing credential relay by an impersonating party.	8	Updated 2026.3				
ISM-1875	Protecting credentials	Networks are scanned at least monthly to identify any credentials that are being stored in the clear.	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5		VPM-06			
ISM-1876	Mitigating known vulnerabilities	Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		VPM-05	ML1	ML2	ML3
ISM-1877	Mitigating known vulnerabilities	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		VPM-05	ML1	ML2	ML3
ISM-1878	Mitigating known vulnerabilities	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	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		VPM-05			
ISM-1879	Mitigating known vulnerabilities	Patches, updates or other vendor mitigations for vulnerabilities in drivers are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		VPM-05			ML3
ISM-1880	Reporting cyber security incidents to customers and the public	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	Subset Of	Incident Stakeholder Reporting	IRO-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	10		IRO-10			
ISM-1881	Reporting cyber security incidents to customers and the public	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	Subset Of	Incident Stakeholder Reporting	IRO-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	10		IRO-10			
ISM-1882	Cyber supply chain risk management activities	Operating systems, applications, IT equipment, OT equipment and services are procured from suppliers that have demonstrated a commitment to transparency for their products and services.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5		TPM-04.1			
ISM-1883	Privileged access to systems	Privileged user accounts explicitly authorised to access online services are strictly limited to only what is required for users and services to undertake their duties.	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5	Updated 2026.3	CFG-03			
ISM-1883	Privileged access to systems	Privileged user accounts explicitly authorised to access online services are strictly limited to only what is required for users and services to undertake their duties.	Functional	Intersects With	Non-Privileged Access for Non-Security Functions	IAC-30.3	Mechanisms exist to prohibit privileged users from using privileged accounts, while performing non-security functions.	8	Updated 2026.3	IAC-21.2			
ISM-1884	Emanation security doctrine	Emanation security doctrine produced by ASD for the management of emanation security matters is complied with.	Functional	No Relationship	N/A	N/A	N/A	0					
ISM-1885	Emanation security risk assessments	Recommended actions contained within emanation security mitigation advice issued for systems are implemented by system owners.	Functional	No Relationship	N/A	N/A	N/A	0					
ISM-1886	Maintaining mobile device security	Mobile devices are configured to operate in a supervised (or equivalent) mode.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-1887	Maintaining mobile device security	Mobile devices are configured with remote locate and wipe functionality.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1888	Maintaining mobile device security	Mobile devices are configured with secure password-based lock screens.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1889	Command Shell	Command line process creation events are centrally logged.	Functional	Intersects With	Event Log & Security-Relevant Telemetry Monitoring	MON-03	Mechanisms exist to review event logs and security-relevant telemetry on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	Updated 2026.3	MON-01.8			
ISM-1889	Command Shell	Command line process creation events are centrally logged.	Functional	Intersects With	Privileged Functions Logging	MON-14	Mechanisms exist to log and review the actions of users and/or services with elevated privileges.	5	Updated 2026.3	MON-03.3			
ISM-1890	Office productivity suites	Microsoft Office macros are checked to ensure they are free of malicious code before being digitally signed or placed within Trusted Locations.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	3	Updated 2026.3	CFG-02			ML3
ISM-1891	Office productivity suites	Microsoft Office macros digitally signed by signatures other than V3 signatures cannot be enabled via the Message Bar or Backstage View.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	3	Updated 2026.3	CFG-02			ML3
ISM-1892	Multi-factor authentication	Multi-factor authentication is used to authenticate users to their organisation's online customer services that process, store or communicate their organisation's sensitive customer data.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5		IAC-06	ML1	ML2	ML3
ISM-1893	Multi-factor authentication	Multi-factor authentication is used to authenticate users to third-party online customer services that process, store or communicate their organisation's sensitive customer data.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5		IAC-06	ML1	ML2	ML3
ISM-1894	Multi-factor authentication	Multi-factor authentication used for authenticating users of data repositories is phishing-resistant.	Functional	Intersects With	Phishing-Resistant Multi-Factor Authentication (MFA)	IAC-37.2	Automated mechanisms exist to enforce phishing-resistant Multi-Factor Authentication (MFA) through authenticators that are cryptographically bound to the verifier's identity, preventing credential relay by an impersonating party.	10	Updated 2026.3				ML3
ISM-1895	Single-factor authentication	Successful and unsuccessful single-factor authentication events are centrally logged.	Functional	Intersects With	Content of Event Logs	MON-09	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5		MON-03			
ISM-1896	Protecting credentials	Memory integrity functionality is enabled.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			ML3
ISM-1897	Protecting credentials	Remote Credential Guard functionality is enabled.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			ML3
ISM-1898	Separate privileged operating environments	Secure Admin Workstations are used in the performance of administrative activities.	Functional	Intersects With	Dedicated Administrative Machines	IAC-27	Mechanisms exist to restrict executing administrative tasks or tasks requiring elevated access to a dedicated machine.	5		IAC-20.4			ML3
ISM-1899	Administrative infrastructure	Network devices that do not belong to administrative infrastructure cannot initiate connections with administrative infrastructure.	Functional	No Relationship	N/A	N/A	N/A	0					
ISM-1900	Vulnerability scanning	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in firmware.	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5		VPM-06			ML3
ISM-1901	Mitigating known vulnerabilities	Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF applications, and security products are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		VPM-05			ML3
ISM-1902	Mitigating known vulnerabilities	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	Updated 2026.3	VPM-05			ML3
ISM-1903	Mitigating known vulnerabilities	Patches, updates or other vendor mitigations for vulnerabilities in firmware are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	Updated 2026.3	VPM-05			ML3
ISM-1904	Mitigating known vulnerabilities	Patches, updates or other vendor mitigations for vulnerabilities in firmware are applied within one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	Updated 2026.3	VPM-05			ML3
ISM-1905	Cessation of support	Online services that are no longer supported by vendors are removed.	Functional	Subset Of	Unsupported Technology Assets, Applications and/or Services (TAAS)	AST-39	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs.	10	Updated 2026.3	TDA-17	ML1	ML2	ML3
ISM-1906	Event log monitoring	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.	Functional	Intersects With	Automated Tools for Real-Time Event Log & Security-Relevant Telemetry Analysis	MON-05.4	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time event log and security-relevant telemetry analysis and incident escalation.	5	Updated 2026.3	MON-01.2			
ISM-1906	Event log monitoring	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.	Functional	Intersects With	Inbound & Outbound Communications Traffic	MON-22	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	5	Updated 2026.3	MON-01.3			
ISM-1907	Event log monitoring	Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events.	Functional	Intersects With	Automated Tools for Real-Time Event Log & Security-Relevant Telemetry Analysis	MON-05.4	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time event log and security-relevant telemetry analysis and incident escalation.	5	Updated 2026.3	MON-01.2			
ISM-1907	Event log monitoring	Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events.	Functional	Intersects With	Inbound & Outbound Communications Traffic	MON-22	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	5	Updated 2026.3	MON-01.3			
ISM-1908	Reporting and resolving vulnerabilities	Vulnerabilities identified in software are publicly disclosed in a responsible and timely manner, including with Common Weakness Enumeration and Common Platform Enumeration information.	Functional	No Relationship	N/A	N/A	N/A	0					
ISM-1909	Reporting and resolving vulnerabilities	In resolving vulnerabilities, root cause analysis is performed and, to the greatest extent possible, entire vulnerability classes are remediated.	Functional	Intersects With	Software Design Root Cause Analysis (RCA)	TDA-05.5	Mechanisms exist to assess software design processes that includes: (1) Conducting Root Cause Analysis (RCA) to identify the underlying causes of issues or failures; (2) Developing actions to address the root cause of the issue or failure; and (3) Implementing the actions and monitoring the implementation for effectiveness.	5		TDA-06.6			
ISM-1910	Network application programming interfaces	Network API calls that facilitate modification of data, or access to data not authorised for release into the public domain, and are accessible over the internet, are centrally logged.	Functional	No Relationship	N/A	N/A	N/A	0					
ISM-1911	Software event logging	Security-relevant usage, error messages and crashes for software are centrally logged.	Functional	Intersects With	Centralized Collection of Event Logs & Security-Relevant Telemetry	MON-05	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of event logs and security-relevant telemetry.	5		MON-02			
ISM-1912	Network documentation	Network documentation includes device settings for all critical servers, high-value servers, network devices and network security appliances.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-09	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and (3) Provides a historical record of applied security controls, including changes.	5		IAO-03			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-1913	Hardening IT equipment configurations	Approved configurations for IT equipment are developed, implemented and maintained.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1914	Hardening operating system configurations	Approved configurations for operating systems are developed, implemented and maintained.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1915	Hardening user application configurations	Approved configurations for user applications are developed, implemented and maintained.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1916	Hardening server application configurations	Approved configurations for server applications are developed, implemented and maintained.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1917	Transitioning to post-quantum cryptography	The development and procurement of new cryptographic equipment, applications and libraries ensures support for the use of ML-DSA-87, ML-KEM-1024, SHA-384, SHA-512 and AES-256 by no later than 2030.	Functional	Intersects With	Post-Quantum Cryptography Agility Plan (PQCAP)	QTS-06	Mechanisms exist to develop a risk-prioritized Post-Quantum Cryptography Agility Plan (PQCAP) that: (1) Enables cryptographic agility; (2) Aligns with evolving security standards; and (3) Defines the approach for selecting and implementing POC algorithms.	5		QTS-03			
ISM-1918	Reporting on cyber security	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-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	5		GOV-01.2			
ISM-1919	Multi-factor authentication	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	No Relationship	N/A	N/A	N/A	0					
ISM-1920	Multi-factor authentication	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	No Relationship	N/A	N/A	N/A	0					
ISM-1921	Vulnerability scanning	The likelihood of system compromise is frequently assessed when working exploits exist for unmitigated vulnerabilities.	Functional	Intersects With	Threat Hunting	THR-13	Mechanisms exist to perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security controls.	5		THR-07			
ISM-1922	Secure mobile application development	The OWASP Mobile Application Security Verification Standard is used in the development of mobile applications.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-05	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5		TDA-06			
ISM-1924	Prompt injection	Generative AI applications evaluate user prompts to detect and mitigate adversarial inputs or suffixes designed to elicit unintended behaviour or assist in the generation of sensitive or harmful content.	Functional	Intersects With	AI Agent Prompt Injection Defense	AAT-39.12	Mechanisms exist to detect and mitigate prompt injection / input attacks that seek to manipulate AI agent instructions, bypass security, compliance and/or resilience controls or result in unauthorized actions.	8		AAT-29.12			
ISM-1926	Microsoft Active Directory services	Microsoft AD DS domain controllers, Microsoft AD CS CA servers, Microsoft AD FS servers and Microsoft Entra Connect servers are only used for their designed role and no other applications or services are installed, unless they are security related.	Functional	Intersects With	Secure Engineering Principles	SEA-05	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	5		SEA-01			
ISM-1927	Microsoft Active Directory services	Access to Microsoft AD DS domain controllers, Microsoft AD CS CA servers, Microsoft AD FS servers and Microsoft Entra Connect servers is limited to privileged users that require access.	Functional	Intersects With	Secure Engineering Principles	SEA-05	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	5		SEA-01			
ISM-1928	Microsoft Active Directory services	Backups of Microsoft AD DS domain controllers, Microsoft AD CS CA servers, Microsoft AD FS servers and Microsoft Entra Connect servers are encrypted using ASD-approved cryptography, stored securely and only accessible to backup administrator accounts.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1928	Microsoft Active Directory services	Backups of Microsoft AD DS domain controllers, Microsoft AD CS CA servers, Microsoft AD FS servers and Microsoft Entra Connect servers are encrypted using ASD-approved cryptography, stored securely and only accessible to backup administrator accounts.	Functional	Intersects With	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5		CRY-01			
ISM-1929	Microsoft Active Directory Domain Services domain controllers	Lightweight Directory Access Protocol signing is enabled on Microsoft AD DS domain controllers.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1930	Microsoft Active Directory Domain Services domain controllers	Passwords are prevented from being stored in Group Policy Preferences.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1931	Microsoft Active Directory Domain Services domain controllers	SID Filtering is enabled for domain and forest trusts.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1932	Microsoft Active Directory Domain Services account hardening	The number of service accounts configured with an SPN is minimised.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1933	Microsoft Active Directory Domain Services account hardening	Service accounts configured with an SPN do not have DCSync permissions.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1934	Microsoft Active Directory Domain Services account hardening	User accounts with DCSync permissions are reviewed at least annually, and those without an ongoing requirement for the permissions have them removed.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1935	Microsoft Active Directory Domain Services account hardening	Computer accounts are not configured for unconstrained delegation.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1936	Microsoft Active Directory Domain Services account hardening	The sIDHistory attribute for user accounts is not used.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1937	Microsoft Active Directory Domain Services account hardening	User accounts are checked at least weekly for the presence of the sIDHistory attribute.	Functional	No Relationship	N/A	N/A	N/A	0					
ISM-1938	Microsoft Active Directory Domain Services account hardening	The Domain Computers security group does not have write or modify permissions to any Microsoft Active Directory objects.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1939	Microsoft Active Directory Domain Services security group memberships	The number of user accounts that are members of the Domain Admins, Enterprise Admins or other highly privileged security groups is minimised.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-10	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5		IAC-16			
ISM-1940	Microsoft Active Directory Domain Services security group memberships	Service accounts are not members of the Domain Admins, Enterprise Admins or other highly privileged security groups.	Functional	Intersects With	Account Management	IAC-08	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and (3) Proactively govern individual, group, system, service, application, guest and temporary accounts.	5		IAC-15			
ISM-1941	Microsoft Active Directory Domain Services security group memberships	Computer accounts are not members of the Domain Admins, Enterprise Admins or other highly privileged security groups.	Functional	Intersects With	Account Management	IAC-08	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and (3) Proactively govern individual, group, system, service, application, guest and temporary accounts.	5		IAC-15			
ISM-1942	Microsoft Active Directory Domain Services security group memberships	The Domain Computers security group is not a member of any privileged or highly privileged security groups.	Functional	Intersects With	Account Management	IAC-08	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and (3) Proactively govern individual, group, system, service, application, guest and temporary accounts.	5		IAC-15			
ISM-1943	Microsoft Active Directory Certificate Services	Strong mapping between certificates and users is enforced.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-1944	Microsoft Active Directory Certificate Services	The EDITF_ATTRIBUTESUBJECTALTNAME2 flag is removed from Microsoft AD CS CA configurations.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1945	Microsoft Active Directory Certificate Services	The CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT flag is removed from certificate templates.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1946	Microsoft Active Directory Certificate Services	Unprivileged user accounts do not have write access to certificate templates.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1947	Microsoft Active Directory Certificate Services	Extended Key Usages that enable user authentication are removed.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1948	Microsoft Active Directory Certificate Services	CA Certificate Manager approval is required for certificate templates that allow a Subject Alternative Name to be supplied.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1949	Microsoft Active Directory Federation Services	Microsoft AD FS servers are administered using a dedicated service account that is not used to administer other systems.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1950	Microsoft Entra Connect	Soft matching between Microsoft AD DS and Microsoft Entra ID is disabled following initial synchronisation activities.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1951	Microsoft Entra Connect	Hard match takeover is disabled for Microsoft Entra Connect servers.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1952	Microsoft Entra Connect	Privileged user accounts are not synchronised between Microsoft AD DS and Microsoft Entra ID.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1953	Setting credentials for built-in Administrator accounts, break glass accounts, local administrator accounts and service accounts	Credentials for the built-in Administrator account in each domain are long, unique, unpredictable and managed.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1954	Setting credentials for built-in Administrator accounts, break glass accounts, local administrator accounts and service accounts	Credentials for built-in Administrator accounts, break glass accounts, local administrator accounts and service accounts are randomly generated.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1955	Changing credentials	Credentials for computer accounts are changed if they are compromised, they are suspected of being compromised or they have not been changed in the past 30 days.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1956	Changing credentials	Microsoft AD FS token-signing and encryption certificates are changed twice in quick succession if they are compromised, they are suspected of being compromised or they have not been changed in the past 12 months.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1957	Protecting credentials	Private keys for Microsoft AD CS CA servers are protected by a hardware security module.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1958	Separate privileged operating environments	User accounts with DCSync permissions cannot logon to unprivileged operating environments.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1959	Event log details	To the extent possible, event logs are captured and stored in a consistent and structured format.	Functional	Intersects With	System Generated Event Logs & Security-Relevant Telemetry	MON-04	Mechanisms exist to generate, monitor, correlate and respond to event logs and security-relevant telemetry from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	5		MON-01.4			
ISM-1960	Event log monitoring	Event logs from internet-facing network devices are analysed in a timely manner to detect cyber security events.	Functional	Intersects With	Centralized Collection of Event Logs & Security-Relevant Telemetry	MON-05	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of event logs and security-relevant telemetry.	5		MON-02			
ISM-1961	Event log monitoring	Event logs from non-internet-facing network devices are analysed in a timely manner to detect cyber security events.	Functional	Intersects With	Correlate Monitoring Information	MON-08	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		MON-02.1			
ISM-1962	Using the Server Message Block protocol	SMB version 1 is not used on networks.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1963	Network device event logging	Security-relevant events for internet-facing network devices are centrally logged.	Functional	Intersects With	Centralized Collection of Event Logs & Security-Relevant Telemetry	MON-05	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of event logs and security-relevant telemetry.	5		MON-02			
ISM-1964	Network device event logging	Security-relevant events for non-internet-facing network devices are centrally logged.	Functional	Intersects With	Correlate Monitoring Information	MON-08	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		MON-02.1			
ISM-1965	Content checking	Files imported or exported via gateways or CDSs undergo content checking.	Functional	Intersects With	DNS & Content Filtering	NET-17	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		NET-18			
ISM-1966	Overseeing the cyber security program	The CISO develops, implements, maintains and regularly verifies a register of systems used by their organisation.	Functional	Intersects With	Asset Inventories	AST-04	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5		AST-02			
ISM-1967	Protecting systems and their resources	System owners, in consultation with each system's authorising officer, ensure controls for each TOP SECRET system and its operating environment, including each sensitive compartmented information system and its operating environment, undergo a security assessment by ASD assessors (or their delegates) to determine if they have been implemented correctly and are operating as intended.	Functional	Intersects With	Control Validation Testing (CVT)	IAO-04	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) 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		IAO-02			
ISM-1968	Protecting systems and their resources	System owners obtain an authorisation to operate for each TOP SECRET system, including for each sensitive compartmented information system, from Director-General ASD (or their delegate).	Functional	Intersects With	Security Authorization	IAO-14	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	5		IAO-07			
ISM-1969	Handling and containing malicious code infections	Malicious code, when stored or communicated, is treated beforehand to prevent accidental execution.	Functional	Intersects With	Malicious Code Protection (Antimalware)	END-04	Mechanisms exist to utilize antimalware, or similar technologies, to detect and eradicate malicious code.	5		END-04			
ISM-1970	Handling and containing malicious code infections	Malicious code processing for cyber security incident response or research purposes is conducted in a dedicated analysis environment segregated from other systems.	Functional	Intersects With	Detonation Chambers (Sandboxes)	IRO-21	Mechanisms exist to utilize a detonation chamber capability to detect and/or block potentially-malicious files and email attachments.	5		IRO-15			
ISM-1971	Assessment of managed service providers	Managed service providers and their TOP SECRET managed services, including sensitive compartmented information managed services, undergo a security assessment by ASD assessors (or their delegates), using the latest release of the ISM available prior to the beginning of the security assessment (or a subsequent release), at least every 24 months.	Functional	Intersects With	Control Validation Testing (CVT)	IAO-04	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) 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		IAO-02			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-1972	Assessment of outsourced cloud service providers	Outsourced cloud service providers and their TOP SECRET cloud services, including sensitive compartmented information cloud services, undergo a security assessment by ASD assessors (or their delegates), using the latest release of the ISM available prior to the beginning of the security assessment (or a subsequent release), at least every 24 months.	Functional	Intersects With	Control Validation Testing (CVT)	IAO-04	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) 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		IAO-02			
ISM-1973	Physical access to systems	Non-classified systems are secured in suitably secure facilities.	Functional	Intersects With	Security of Assets & Media	AST-18	Mechanisms exist to maintain strict control over Technology Assets, Applications, Services and/or Data (TAASD) to preserve confidentiality and integrity.	5		AST-05			
ISM-1974	Physical access to servers, network devices and cryptographic equipment	Non-classified servers, network devices and cryptographic equipment are secured in suitably secure server rooms or communications rooms.	Functional	Intersects With	Technology Assets, Applications, Services and/or Data (TAASD) Storage	AST-19	Mechanisms exist to ensure Technology Assets, Applications, Services and/or Data (TAASD) are stored in rooms and/or facilities with reasonable physical security protections.	5		AST-05.2			
ISM-1975	Physical access to servers, network devices and cryptographic equipment	Non-classified servers, network devices and cryptographic equipment are secured in suitably secure security containers.	Functional	Intersects With	Technology Assets, Applications, Services and/or Data (TAASD) Storage	AST-19	Mechanisms exist to ensure Technology Assets, Applications, Services and/or Data (TAASD) are stored in rooms and/or facilities with reasonable physical security protections.	5		AST-05.2			
ISM-1976	Operating system event logging	Security-relevant events for Apple macOS operating systems are centrally logged.	Functional	Intersects With	Centralized Collection of Event Logs & Security-Relevant Telemetry	MON-05	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of event logs and security-relevant telemetry.	5		MON-02			
ISM-1977	Operating system event logging	Security-relevant events for Linux operating systems are centrally logged.	Functional	Intersects With	Centralized Collection of Event Logs & Security-Relevant Telemetry	MON-05	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of event logs and security-relevant telemetry.	5		MON-02			
ISM-1978	Server application event logging	Security-relevant events for server applications on internet-facing servers are centrally logged.	Functional	Intersects With	Centralized Collection of Event Logs & Security-Relevant Telemetry	MON-05	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of event logs and security-relevant telemetry.	5		MON-02			
ISM-1979	Server application event logging	Security-relevant events for server applications on non-internet-facing servers are centrally logged.	Functional	Intersects With	Centralized Collection of Event Logs & Security-Relevant Telemetry	MON-05	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of event logs and security-relevant telemetry.	5		MON-02			
ISM-1980	Protecting credentials	Credential hint functionality is not used for systems.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1980	Protecting credentials	Credential hint functionality is not used for systems.	Functional	Intersects With	Password-Based Authentication	IAC-15	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5		IAC-10.1			
ISM-1981	Cessation of support	Non-internet-facing network devices that are no longer supported by vendors are replaced.	Functional	Intersects With	Unsupported Technology Assets, Applications and/or Services (TAAS)	AST-39	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs.	5		TDA-17			
ISM-1982	Cessation of support	Networked IT equipment that is no longer supported by vendors is replaced.	Functional	Intersects With	Unsupported Technology Assets, Applications and/or Services (TAAS)	AST-39	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs.	5		TDA-17			
ISM-1983	Centralised event logging facility	Event logs sent to a centralised event logging facility are sent as soon as possible after they occur.	Functional	Intersects With	Centralized Collection of Event Logs & Security-Relevant Telemetry	MON-05	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of event logs and security-relevant telemetry.	5		MON-02			
ISM-1984	Centralised event logging facility	Event logs sent to a centralised event logging facility are encrypted in transit using Australian Signals Directorate (ASD)-approved cryptography.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-1984	Centralised event logging facility	Event logs sent to a centralised event logging facility are encrypted in transit using Australian Signals Directorate (ASD)-approved cryptography.	Functional	Intersects With	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5		CRY-01			
ISM-1984	Centralised event logging facility	Event logs sent to a centralised event logging facility are encrypted in transit using Australian Signals Directorate (ASD)-approved cryptography.	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03			
ISM-1985	Centralised event logging facility	Event logs are protected from unauthorised access.	Functional	Intersects With	Protection of Event Logs & Security-Relevant Telemetry	MON-12	Mechanisms exist to protect event logs, security-relevant telemetry and audit tools from unauthorized access, modification and deletion.	8	Updated 2026.3	MON-08			
ISM-1985	Centralised event logging facility	Event logs are protected from unauthorised access.	Functional	Intersects With	Event Log & Security-Relevant Telemetry Access by Subset of	MON-12.2	Mechanisms exist to restrict access to the management of event logs and security-relevant telemetry to privileged users with a specific business need.	5		MON-08.2			
ISM-1986	Event log monitoring	Event logs from critical servers are analysed in a timely manner to detect cyber security events.	Functional	Intersects With	Event Log & Security-Relevant Telemetry Monitoring	MON-03	Mechanisms exist to review event logs and security-relevant telemetry on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	Updated 2026.3	MON-01.8			
ISM-1986	Event log monitoring	Event logs from critical servers are analysed in a timely manner to detect cyber security events.	Functional	Intersects With	Centralized Collection of Event Logs & Security-Relevant Telemetry	MON-05	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of event logs and security-relevant telemetry.	5		MON-02			
ISM-1987	Event log monitoring	Event logs from security products are analysed in a timely manner to detect cyber security events.	Functional	Intersects With	Event Log & Security-Relevant Telemetry Monitoring	MON-03	Mechanisms exist to review event logs and security-relevant telemetry on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	Updated 2026.3	MON-01.8			
ISM-1987	Event log monitoring	Event logs from security products are analysed in a timely manner to detect cyber security events.	Functional	Intersects With	Centralized Collection of Event Logs & Security-Relevant Telemetry	MON-05	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of event logs and security-relevant telemetry.	5		MON-02			
ISM-1988	Event log retention	Event logs are retained in a searchable manner for at least 12 months.	Functional	Intersects With	Event Log & Security-Relevant Telemetry Retention	MON-13	Mechanisms exist to retain event logs and security-relevant telemetry 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		MON-10			
ISM-1989	Event log retention	Event logs are retained as per minimum retention requirements for various classes of records as set out by the National Archives of Australia's Administrative Functions Disposal Authority Express (AFDA Express) Version 2 publication.	Functional	Intersects With	Event Log & Security-Relevant Telemetry Retention	MON-13	Mechanisms exist to retain event logs and security-relevant telemetry 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		MON-10			
ISM-1990	Using post-quantum cryptographic algorithms	When using ML-DSA and ML-KEM, as per FIPS 204 and FIPS 203 respectively, adherence to pre-requisite FIPS 140-3 validation is preferred.	Functional	Intersects With	Approved Post-Quantum Cryptography (PQC) Algorithm Use	QTS-09.3	Mechanisms exist to define: (1) Approved Post-Quantum Cryptography (PQC) algorithms, including asymmetric and symmetric algorithms; and (2) Required validation levels for approved algorithms (e.g., FIPS 140-3 validated).	5		QTS-06.3			
ISM-1991	Using the Module-Lattice-Based Digital Signature Algorithm	When using ML-DSA for digital signatures, ML-DSA-65 or ML-DSA-87 is used, preferably ML-DSA-87.	Functional	Intersects With	Approved Post-Quantum Cryptography (PQC) Algorithm Use	QTS-09.3	Mechanisms exist to define: (1) Approved Post-Quantum Cryptography (PQC) algorithms, including asymmetric and symmetric algorithms; and (2) Required validation levels for approved algorithms (e.g., FIPS 140-3 validated).	5		QTS-06.3			
ISM-1992	Using the Module-Lattice-Based Digital Signature Algorithm	When using ML-DSA for digital signatures, the hedged variant is used whenever possible.	Functional	Intersects With	Approved Post-Quantum Cryptography (PQC) Algorithm Use	QTS-09.3	Mechanisms exist to define: (1) Approved Post-Quantum Cryptography (PQC) algorithms, including asymmetric and symmetric algorithms; and (2) Required validation levels for approved algorithms (e.g., FIPS 140-3 validated).	5		QTS-06.3			
ISM-1993	Using the Module-Lattice-Based Digital Signature Algorithm	Pre-hashed variants of ML-DSA-65 and ML-DSA-87 are only used when the performance of default variants is unacceptable.	Functional	Intersects With	Approved Post-Quantum Cryptography (PQC) Algorithm Use	QTS-09.3	Mechanisms exist to define: (1) Approved Post-Quantum Cryptography (PQC) algorithms, including asymmetric and symmetric algorithms; and (2) Required validation levels for approved algorithms (e.g., FIPS 140-3 validated).	5		QTS-06.3			
ISM-1994	Using the Module-Lattice-Based Digital Signature Algorithm	When the pre-hashed variants of ML-DSA-65 and ML-DSA-87 are used, at least SHA-384 and SHA-512 respectively are used for pre-hashing.	Functional	Intersects With	Approved Post-Quantum Cryptography (PQC) Algorithm Use	QTS-09.3	Mechanisms exist to define: (1) Approved Post-Quantum Cryptography (PQC) algorithms, including asymmetric and symmetric algorithms; and (2) Required validation levels for approved algorithms (e.g., FIPS 140-3 validated).	5		QTS-06.3			
ISM-1995	Using the Module-Lattice-Based Key Encapsulation Mechanism	When using ML-KEM for encapsulating encryption session keys (and similar keys), ML-KEM-768 or ML-KEM-1024 is used, preferably ML-KEM-1024.	Functional	Intersects With	Approved Post-Quantum Cryptography (PQC) Algorithm Use	QTS-09.3	Mechanisms exist to define: (1) Approved Post-Quantum Cryptography (PQC) algorithms, including asymmetric and symmetric algorithms; and (2) Required validation levels for approved algorithms (e.g., FIPS 140-3 validated).	5		QTS-06.3			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-1996	Post-quantum traditional hybrid schemes	When a post-quantum traditional hybrid scheme is used, either the post-quantum cryptographic algorithm, the traditional cryptographic algorithm or both are AACAs.	Functional	Intersects With	Hybrid / Composite Cryptography	QTS-09.9	Mechanisms exist to leverage hybrid/composite algorithms as a transition path to Post-Quantum Cryptography (PQC) solutions that: (1) Support hybrid signatures (e.g., ECDSA + ML-DSA) and hybrid Key Encapsulation Mechanisms (KEMs) (e.g., ECDH + ML-KEM); (2) Ensure certificate formats, Public Key Infrastructure (PKI) and trust anchors can support dual-key or dual-certificate models; and (3) Plan for eventual removal of classical algorithms once PQC confidence is sufficient.	5		QTS-06.9			
ISM-1997	Embedding cyber security	The board of directors or executive committee defines clear roles and responsibilities for cyber security both within the board of directors or executive committee and broadly within their organisation.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-05	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 Security, Compliance & Resilience Program (SCRP).	5		GOV-04			
ISM-1998	Embedding cyber security	The board of directors or executive committee ensures that cyber security is integrated throughout all business functions within their organisation.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-09	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5		GOV-01.1			
ISM-1999	Embedding cyber security	The board of directors or executive committee ensures the cyber security strategy for their organisation is aligned with the overarching strategic direction and business strategy for their organisation.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-09	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5		GOV-01.1			
ISM-2000	Embedding cyber security	The board of directors or executive committee seeks regular briefings or reporting on the cyber security posture of their organisation, as well as the threat environment in which they operate, from internal and external subject matter experts.	Functional	Intersects With	Status Reporting To Governing Body	GOV-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	5		GOV-01.2			
ISM-2001	Championing a positive cyber security culture	The board of directors or executive committee champions a positive cyber security culture within their organisation, including through leading by example.	Functional	Intersects With	Business As Usual (BAU) Security, Compliance & Resilience Practices	GOV-10	Mechanisms exist to incorporate security, compliance and resilience principles into Business As Usual (BAU) practices through executive leadership involvement.	5		GOV-14			
ISM-2002	Building cyber security expertise	The board of directors or executive committee maintains a sufficient level of cyber security literacy to fulfil both their fiduciary duties and any legislative or regulatory obligations.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-09	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5		GOV-01.1			
ISM-2003	Building cyber security expertise	The board of directors or executive committee maintains awareness of key cyber security recruitment activities, retention rates for cyber security personnel, and cyber security skills and experience gaps within their organisation.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-09	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5		GOV-01.1			
ISM-2004	Building cyber security expertise	The board of directors or executive committee supports the development of cyber security skills and experience for all personnel via internal and external cyber security awareness raising and training opportunities.	Functional	Intersects With	Security, Compliance & Resilience Resource Management	PRM-05	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions.	5		PRM-02			
ISM-2005	Identifying critical business assets	The board of directors or executive committee understands the business criticality of their organisation's systems, including at least a basic understanding of what systems exist, their value, where they reside, who has access, who might seek access, how they are protected, and how that protection is verified.	Functional	Intersects With	Identify Critical Assets	AST-05	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	5		BCD-02			
ISM-2005	Identifying critical business assets	The board of directors or executive committee understands the business criticality of their organisation's systems, including at least a basic understanding of what systems exist, their value, where they reside, who has access, who might seek access, how they are protected, and how that protection is verified.	Functional	Intersects With	High Value Assets (HVAs)	GOV-08	Mechanisms exist to identify and catalog the organization's High Value Assets (HVAs) (e.g., crown jewels), including defining: (1) Criteria for high-value Intellectual Property (IP) to be categorized as a HVA; (2) Criteria for Technology Assets, Applications and Services (TAAS) to be categorized as a HVA based on business process criticality or dependency relationships; (3) Location of HVA Technology Assets, Applications, Services and/or Data (TAASD); (4) Assigned owners; (5) Minimum protection mechanisms that must be implemented; and (6) Assurance requirements.	5		GOV-21			
ISM-2005	Identifying critical business assets	The board of directors or executive committee understands the business criticality of their organisation's systems, including at least a basic understanding of what systems exist, their value, where they reside, who has access, who might seek access, how they are protected, and how that protection is verified.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-09	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5		GOV-01.1			
ISM-2005	Identifying critical business assets	The board of directors or executive committee understands the business criticality of their organisation's systems, including at least a basic understanding of what systems exist, their value, where they reside, who has access, who might seek access, how they are protected, and how that protection is verified.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-09	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and (3) Provides a historical record of applied security controls, including changes.	5		IAO-03			
ISM-2006	Planning for major cyber security incidents	The board of directors or executive committee plans for major cyber security incidents, including by participating in exercises, and understands their duties in relation to such cyber security incidents.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-09	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5		GOV-01.1			
ISM-2006	Planning for major cyber security incidents	The board of directors or executive committee plans for major cyber security incidents, including by participating in exercises, and understands their duties in relation to such cyber security incidents.	Functional	Intersects With	Incident Response Capabilities Testing	IRO-09	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5		IRO-06			
ISM-2007	Bringing medical devices into facilities	An authorised medical device register for SECRET and TOP SECRET areas is developed, implemented, maintained and regularly verified.	Functional	No Relationship	N/A	N/A	N/A	0					
ISM-2008	Bringing medical devices into facilities	Medical devices authorised to be brought into SECRET and TOP SECRET areas meet, at a minimum, the following criteria: • are listed on the Australian Register of Therapeutic Goods • have been prescribed by a legally qualified medical practitioner • have been commercially purchased within Australia • do not have inbuilt cellular connectivity • can operate independently of mobile devices • where possible, have Wi-Fi, Bluetooth and other forms of wireless connectivity disabled when operating within SECRET and TOP SECRET areas.	Functional	No Relationship	N/A	N/A	N/A	0					
ISM-2009	Bringing medical devices into facilities	Unauthorised medical devices are not brought into SECRET and TOP SECRET areas.	Functional	No Relationship	N/A	N/A	N/A	0					
ISM-2010	Microsoft Active Directory Domain Services account hardening	Service accounts configured with an SPN use the Advanced Encryption Standard for encryption.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-2011	Multi-factor authentication	When phishing-resistant multi-factor authentication is used by user accounts, other non-phishing-resistant multi-factor authentication options are disabled for such user accounts.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5		IAC-06			
ISM-2011	Multi-factor authentication	When phishing-resistant multi-factor authentication is used by user accounts, other non-phishing-resistant multi-factor authentication options are disabled for such user accounts.	Functional	Intersects With	Phishing-Resistant Multi-Factor Authentication (MFA)	IAC-37.2	Automated mechanisms exist to enforce phishing-resistant Multi-Factor Authentication (MFA) through authenticators that are cryptographically bound to the verifier's identity, preventing credential relay by an impersonating party.	8	Updated 2026.3				
ISM-2012	Screen locking	Systems are configured with a screen lock that: • activates after a maximum of 15 minutes of user inactivity, or when manually activated by users • conceals all content on the screen • ensures that the screen does not enter a power saving state before the screen lock is activated • requires users to re-authenticate using all authentication factors to unlock the system • denies users the ability to disable the screen locking mechanism.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-2013	Network application programming interfaces	Authentication and authorisation of clients is performed when clients call network APIs that facilitate modification of data but are not accessible over the internet.	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-03	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	3		IAC-01.2			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-2014	Network application programming interfaces	Authentication and authorisation of clients is performed when clients call network APIs that facilitate access to data not authorised for release into the public domain but are not accessible over the internet.	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-03	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	3		IAC-01.2			
ISM-2015	Network application programming interfaces	Network API calls that facilitate modification of data, or access to data not authorised for release into the public domain, but are not accessible over the internet, are centrally logged.	Functional	Intersects With	Inbound & Outbound Communications Traffic	MON-22	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	5		MON-01.3			
ISM-2016	Software input handling	Validation and sanitisation are performed on all input received over a local network by software.	Functional	Intersects With	Web Application Input Validation & Sanitization	WEB-08	Mechanisms exist to ensure all input handled by a web application is validated and/or sanitized.	5	Updated 2026.3	WEB-09			
ISM-2017	Encrypted Domain Name System Services	DNS traffic is encrypted by clients and servers using ASD-approved cryptography.	Functional	Intersects With	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5		CRY-01			
ISM-2017	Encrypted Domain Name System Services	DNS traffic is encrypted by clients and servers using ASD-approved cryptography.	Functional	Intersects With	Domain Name Service (DNS) Resolution	NET-13	Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.	5		NET-10			
ISM-2018	Border Gateway Protocol routing security	Routes for RPKI-registered IP addresses that are advertised from invalid Autonomous Systems, or that are longer than allowed, are rejected or deprioritised by routers that exchange routes via BGP.	Functional	No Relationship	N/A	N/A	N/A	0					
ISM-2019	Assessment of gateways	TOP SECRET gateways undergo a security assessment by ASD assessors (or their delegates), using the latest release of the ISM available prior to the beginning of the assessment (or a subsequent release), at least every 24 months.	Functional	Intersects With	Specialized Assessments	IAO-05	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 and OT); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; (11) Artificial Intelligence and Autonomous Technologies (AAT); and/or (12) Other Technology Assets, Applications and/or Services (TAAS) that require specialized expertise to determine conformity with security, compliance and/or resilience requirements.	5		IAO-02.2			
ISM-2020	Overseeing cyber security personnel	The CISO ensures sufficient cyber security personnel, with the right skills and experience, are acquired to support cyber security activities within their organisation.	Functional	Intersects With	Prioritization To Address Evolving Risks & Threats	PRM-05.2	Mechanisms exist to integrate foundational cybersecurity practices with advanced technologies to maintain situation awareness of and minimize the organization's exposure to evolving risks and threats.	5		PRM-02.1			
ISM-2020	Overseeing cyber security personnel	The CISO ensures sufficient cyber security personnel, with the right skills and experience, are acquired to support cyber security activities within their organisation.	Functional	Intersects With	Allocation of Resources	PRM-06	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	5		PRM-03			
ISM-2021	Protecting systems and their resources	System owners implement and maintain data minimisation practices for each of their systems.	Functional	Intersects With	Minimize Sensitive / Regulated Data Exposure	DCH-27.1	Mechanisms exist to minimize sensitive and/or regulated data that is collected, received, processed, stored and/or transmitted throughout the information lifecycle to only those elements necessary to support necessary business processes.	5		DCH-18.1			
ISM-2022	Providing cyber security awareness training	A cyber security awareness training register is developed, implemented and maintained.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-02	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10		SAT-01			
ISM-2023	Authoritative source for software	An authoritative source for software is established and maintained.	Functional	Intersects With	Production Software Repository	CFG-17	Mechanisms exist to maintain an authoritative repository for production software.	5		CFG-09			
ISM-2024	Authoritative source for software	The authoritative source for software is used for all software development activities.	Functional	Intersects With	Software Development Repository	CFG-17.3	Mechanisms exist to maintain an authoritative repository for software development activities that is separate from production software.	5		CFG-09.3			
ISM-2025	Issue tracking	An issue tracking solution is used to link software development tasks to security issues and decisions, change or feature requests, programming issues, or bug fixes.	Functional	Subset Of	Software Assurance Maturity Model (SAMM)	TDA-03.1	Mechanisms exist to utilize a Software Assurance Maturity Model (SAMM) to govern a secure development lifecycle for the development of Technology Assets, Applications and/or Services (TAAS).	10		TDA-06.3			
ISM-2026	Software artefacts	All software artefacts are scanned for malicious content before being imported into the authoritative source for software.	Functional	Intersects With	Software Repository Protections	CFG-17.2	Mechanisms exist to protect software repositories from importing untrusted and/or malicious software artifacts by: (1) Scanning artifacts for malicious content; (2) Verifying a digital signature or secure hash provided over a secure channel; and (3) Scanning artifacts to identify plain text or encoded secrets and keys.	5		CFG-09.2			
ISM-2027	Software artefacts	All software artefacts are verified by a digital signature, or a secure hash provided over a secure channel, before being imported into the authoritative source for software.	Functional	Intersects With	Software Repository Protections	CFG-17.2	Mechanisms exist to protect software repositories from importing untrusted and/or malicious software artifacts by: (1) Scanning artifacts for malicious content; (2) Verifying a digital signature or secure hash provided over a secure channel; and (3) Scanning artifacts to identify plain text or encoded secrets and keys.	5		CFG-09.2			
ISM-2028	Software artefacts	All software artefacts are tested to detect known weaknesses using static application security testing (SAST), dynamic application security testing (DAST) or software composition analysis (SCA), depending on the software artefact type, before being imported into the authoritative source for software.	Functional	Intersects With	Static Code Analysis	TDA-17.1	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ static code analysis tools to identify and remediate common flaws and document the results of the analysis.	5		TDA-09.2			
ISM-2028	Software artefacts	All software artefacts are tested to detect known weaknesses using static application security testing (SAST), dynamic application security testing (DAST) or software composition analysis (SCA), depending on the software artefact type, before being imported into the authoritative source for software.	Functional	Intersects With	Dynamic Code Analysis	TDA-17.2	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ dynamic code analysis tools to identify and remediate common flaws and document the results of the analysis.	5		TDA-09.3			
ISM-2029	Software artefacts	The authoritative source for software restricts the use and import of third-party libraries and software components to trustworthy sources.	Functional	Intersects With	Third-Party Libraries	CFG-17.1	Mechanisms exist to restrict the use and import of third-party libraries and/or software components to trustworthy sources.	5		CFG-09.1			
ISM-2030	Software artefacts	Scanning is used during commits to identify plain text or encoded secrets and keys, which are then blocked from being stored in the authoritative source for software.	Functional	Intersects With	Software Repository Protections	CFG-17.2	Mechanisms exist to protect software repositories from importing untrusted and/or malicious software artifacts by: (1) Scanning artifacts for malicious content; (2) Verifying a digital signature or secure hash provided over a secure channel; and (3) Scanning artifacts to identify plain text or encoded secrets and keys.	5		CFG-09.2			
ISM-2031	Build solution	Compilers, interpreters and build tools (including pipelines) that provide security features to improve executable file security are implemented and such security features are used.	Functional	Intersects With	Supporting Toolchain	TDA-05.3	Automated mechanisms exist to improve the accuracy, consistency and comprehensiveness of secure practices throughout the asset's lifecycle.	3		TDA-06.4			
ISM-2032	Build solution	The build solution ensures that all automated testing is completed without warnings, alerts or errors before building software artefacts.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-05	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5		TDA-06			
ISM-2033	Secure software development	All software security requirements are documented, stored securely and maintained throughout the software development life cycle.	Functional	Intersects With	Developer Architecture & Design	TDA-04	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a design specification and security architecture that: (1) Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture; (2) Accurately and completely describes the required security functionality and the allocation of security, compliance and resilience controls among physical and logical components; and (3) Expresses how individual security functions, mechanisms and services work together to provide required security capabilities and a unified approach to protection.	5		TDA-05			
ISM-2034	Secure software development	Security design decisions are documented and reviewed throughout the software development cycle.	Functional	Intersects With	Software Assurance Maturity Model (SAMM)	TDA-03.1	Mechanisms exist to utilize a Software Assurance Maturity Model (SAMM) to govern a secure development lifecycle for the development of Technology Assets, Applications and/or Services (TAAS).	5		TDA-06.3			
ISM-2035	Secure software development	Security roles, responsibilities and knowledge required to support the software development life cycle are identified and documented.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-04	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5		HRS-03			
ISM-2035	Secure software development	Security roles, responsibilities and knowledge required to support the software development life cycle are identified and documented.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-05	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5		TDA-06			
ISM-2036	Secure software development	Security responsibilities for software developers are identified and documented.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-04	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5		HRS-03			
ISM-2037	Secure software development	Software developers that lack sufficient cyber security knowledge and skills required for their projects or tasks undertake suitable training or upskilling on secure software development and programming practices.	Functional	Intersects With	Requisite Developer Training	TDA-19.2	Mechanisms exist to ensure developers of Technology Assets, Applications and/or Services (TAAS) who lack the requisite skillset receive suitable training on Secure Software Development Practices (SSDP).	5		TDA-13.2			
ISM-2038	Secure software development	A software developer cyber security knowledge and skills register is implemented and maintained.	Functional	Intersects With	Developer Knowledge & Skills Register	TDA-19.1	Mechanisms exist to maintain a cybersecurity knowledge and skills register for developers.	5		TDA-13.1			
ISM-2039	Secure software development	The software threat model is reviewed throughout the software development life cycle to ensure it reflects the as-built software and any changes to the threat environment.	Functional	Intersects With	Threat Modeling	TDA-05.2	Mechanisms exist to perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.	5		TDA-06.2			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-2040	Secure software development	Secure programming practices for the chosen programming language are used for software development.	Functional	Intersects With	Programming Language Selection	TDA-04.1	Mechanisms exist to: (1) Define organization-approved programming language(s) for software development; and (2) Document the justification for selection decisions.	5		TDA-06.7			
ISM-2041	Secure software development	Memory-safe programming languages, or less preferably memory-safe programming practices, are used for software development.	Functional	Intersects With	Programming Language Selection	TDA-04.1	Mechanisms exist to: (1) Define organization-approved programming language(s) for software development; and (2) Document the justification for selection decisions.	5		TDA-06.7			
ISM-2041	Secure software development	Memory-safe programming languages, or less preferably memory-safe programming practices, are used for software development.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-05	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5		TDA-06			
ISM-2042	Secure software development	Secure by Default principles and practices are followed throughout the software development life cycle, including by ensuring that all built-in security measures are included and enabled in the base product at no extra cost to consumers.	Functional	Intersects With	Secure Settings By Default	TDA-03.2	Mechanisms exist to implement secure configuration settings by default to reduce the likelihood of Technology Assets, Applications and/or Services (TAAS) being deployed with weak security settings that would put the TAAS at a greater risk of compromise.	5		TDA-09.6			
ISM-2043	Secure software development	Software is architected and structured to support readability and maintainability.	Functional	Intersects With	Developer Architecture & Design	TDA-04	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a design specification and security architecture that: (1) Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture; (2) Accurately and completely describes the required security functionality and the allocation of security, compliance and resilience controls among physical and logical components; and (3) Expresses how individual security functions, mechanisms and services work together to provide required security capabilities and a unified approach to protection.	5		TDA-05			
ISM-2044	Secure software development	Software has no default credentials; however, if credentials are required, they are created on first install by the installing organisation.	Functional	Intersects With	Default Authenticators	IAC-14.4	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	5		IAC-10.8			
ISM-2044	Secure software development	Software has no default credentials; however, if credentials are required, they are created on first install by the installing organisation.	Functional	Intersects With	Secure Settings By Default	TDA-03.2	Mechanisms exist to implement secure configuration settings by default to reduce the likelihood of Technology Assets, Applications and/or Services (TAAS) being deployed with weak security settings that would put the TAAS at a greater risk of compromise.	5		TDA-09.6			
ISM-2045	Secure software development	Application backwards compatibility does not compromise any security measures or features.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-05	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5		TDA-06			
ISM-2046	Secure software development	Where software allows user impersonation, sensitive data is not logged and appropriate permissions are set.	Functional	No Relationship	N/A	N/A	N/A	0					
ISM-2048	Secure software development	Where software supports multiple user roles, non-administrative users are prevented from altering their profile permissions or privileges.	Functional	Intersects With	Prohibit Non-Privileged Users from Executing Privileged Functions	IAC-30.1	Mechanisms exist to prevent non-privileged users from executing privileged functions to include disabling, circumventing or altering implemented security safeguards / countermeasures.	5		IAC-21.5			
ISM-2050	Secure software development	When digital signatures are processed by software, they are validated against a certificate trust chain and checked for revocation using a Certificate Revocation List or with the Online Certificate Status Protocol.	Functional	Intersects With	Public Key Infrastructure (PKI)	CRY-09	Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service provider.	5		CRY-08			
ISM-2051	Secure software development	Software generates sufficient event logs to support the detection of cyber security events.	Functional	Intersects With	Content of Event Logs	MON-09	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5		MON-03			
ISM-2052	Secure software development	Event logs produced by software ensure that any sensitive data is protected.	Functional	Intersects With	Sensitive Event Log & Security-Relevant Telemetry Data	MON-30	Mechanisms exist to protect sensitive and/or regulated data contained in event logs and security-relevant telemetry.	5		MON-03.1			
ISM-2053	Secure software development	End of life procedures for software, including procedures for software removal and the archival or destruction of user accounts and data, are produced and made available to consumers.	Functional	Intersects With	Decommissioning	AST-36	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are properly decommissioned so that: (1) Data is properly transitioned to new systems or archived; and (2) Hard drives are either destroyed or erased in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5		AST-30			
ISM-2054	Software bill of materials	If a software bill of materials is available for imported third-party software components, it is used during software development to ensure such software components have no known vulnerabilities.	Functional	Intersects With	Software Bill of Materials (SBOM)	TDA-21.4	Mechanisms exist to generate, or obtain, a Software Bill of Materials (SBOM) for Technology Assets, Applications and/or Services (TAAS) that lists software packages in use, including versions and applicable licenses.	5		TDA-04.2			
ISM-2055	Software build provenance	If a software build provenance is available for imported third-party software components, it is used during software development to ensure such software components are built to an appropriate standard.	Functional	No Relationship	N/A	N/A	N/A	0					
ISM-2056	Software build provenance	A software build provenance is produced and made available to consumers of software.	Functional	Intersects With	Software Bill of Materials (SBOM)	TDA-21.4	Mechanisms exist to generate, or obtain, a Software Bill of Materials (SBOM) for Technology Assets, Applications and/or Services (TAAS) that lists software packages in use, including versions and applicable licenses.	5		TDA-04.2			
ISM-2057	Software input handling	All input validation rules are documented, implemented in code, and tested using both positive and negative unit tests and integration tests.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-17	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience 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 control testing and evaluation process; and (3) Document the results.	5		TDA-09			
ISM-2057	Software input handling	All input validation rules are documented, implemented in code, and tested using both positive and negative unit tests and integration tests.	Functional	Intersects With	Malformed Input Testing	TDA-17.3	Mechanisms exist to utilize testing methods to ensure Technology Assets, Applications and/or Services (TAAS) continue to operate as intended when subject to invalid or unexpected inputs on its interfaces.	5		TDA-09.4			
ISM-2058	Software input handling	Data sources and serialised data inputs are validated before being deserialised.	Functional	Intersects With	Web Application Input Validation & Sanitization	WEB-08	Mechanisms exist to ensure all input handled by a web application is validated and/or sanitized.	5	Updated 2026.3	WEB-09			
ISM-2059	Software input handling	File uploads or input are restricted to specific file types, with malicious content scanning occurring prior to file access, file execution or file storage.	Functional	Intersects With	Input Data Validation	TDA-12	Mechanisms exist to check the validity of information inputs.	5		TDA-18			
ISM-2060	Software security testing	Code reviews are utilised to ensure software components meets Secure by Design principles and practices as well as secure programming practices.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-17	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience 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 control testing and evaluation process; and (3) Document the results.	5		TDA-09			
ISM-2061	Software security testing	Peer reviews are conducted on all critical and security-related software components.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-17	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience 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 control testing and evaluation process; and (3) Document the results.	5		TDA-09			
ISM-2062	Software security testing	Unit testing and integration testing, covering both positive and negative use cases, are used for software components to ensure code quality and correctness.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-17	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience 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 control testing and evaluation process; and (3) Document the results.	5		TDA-09			
ISM-2063	Secure web application design and development	If supported, web application session cookies set the HttpOnly flag, Secure flag and the SameSite flag by default.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-05	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5		TDA-06			
ISM-2064	Secure web application design and development	Web application session cookies contain only digitally signed opaque bearer tokens.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-05	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5		TDA-06			
ISM-2065	Secure web application design and development	Web application session cookies using opaque bearer tokens that are not digitally signed use non-sequential random identifiers with a minimum of 128 bits of entropy, preferably 256 bits of entropy.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-05	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5		TDA-06			
ISM-2066	Secure web application design and development	Web application sessions are centrally managed server side.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-05	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5		TDA-06			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-2067	Secure web application design and development	Web applications that support Single Sign On equally support Single Logout.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-05	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5		TDA-06			
ISM-2068	Functional separation between networked devices and the internet	Internet connectivity for networked devices is strictly limited to those that require access.	Functional	Intersects With	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all and permit by exception).	5		NET-04.1			
ISM-2069	Bringing photographic and video recording devices into facilities	An authorised photographic and video recording device register for SECRET and TOP SECRET areas is developed, implemented, maintained and regularly verified.	Functional	No Relationship	N/A	N/A	N/A	0					
ISM-2070	Bringing photographic and video recording devices into facilities	Unauthorised photographic and video recording devices are not brought into SECRET and TOP SECRET areas.	Functional	No Relationship	N/A	N/A	N/A	0					
ISM-2071	Managing and reporting suspicious requests to disclose or change user account details	Personnel dealing with user account details are advised of what social engineering attacks are, how to manage such situations and how to report them.	Functional	Intersects With	Social Engineering & Mining	SAT-06.1	Mechanisms exist to include awareness training on recognizing and reporting potential and actual instances of social engineering and social mining.	5		SAT-02.2			
ISM-2072	Secure artificial intelligence application development	AI models are stored in a non-executable file format that does not allow arbitrary code execution.	Functional	Intersects With	Artificial Intelligence (AI) & Autonomous Technologies Governance	AAT-02	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.	5		AAT-01			
ISM-2073	Transitioning to post-quantum cryptography	A post-quantum cryptography transition plan is developed, implemented and maintained.	Functional	Intersects With	Post-Quantum Cryptography Agility Plan (PQCAP)	QTS-06	Mechanisms exist to develop a risk-prioritized Post-Quantum Cryptography Agility Plan (PQCAP) that: (1) Enables cryptographic agility; (2) Aligns with evolving security standards; and (3) Defines the approach for selecting and implementing PQC algorithms.	8		QTS-03			
ISM-2074	General-purpose artificial intelligence usage policy	A general-purpose AI usage policy is developed, implemented and maintained.	Functional	Subset Of	Artificial Intelligence & Autonomous Technologies Policy	AAT-01	Mechanisms exist to establish a formal, documented Artificial Intelligence and Autonomous Technologies (AAT) policy that: (1) Conveys executive management's intent; (2) Provides organizational direction and expected	10	Updated 2026.3				
ISM-2074	General-purpose artificial intelligence usage policy	A general-purpose AI usage policy is developed, implemented and maintained.	Functional	Intersects With	Artificial Intelligence (AI) & Autonomous Technologies Governance	AAT-02	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	8		AAT-01			
ISM-2074	General-purpose artificial intelligence usage policy	A general-purpose AI usage policy is developed, implemented and maintained.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10		GOV-02			
ISM-2075	Sending and receiving fax messages	Fax machines, and online fax services, are not used for sending or receiving fax messages.	Functional	Intersects With	Technology Use Restrictions	HRS-06.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	5		HRS-05.3			
ISM-2076	Insecure authentication methods	Security questions are not used for authentication purposes.	Functional	Intersects With	Identity & Access Management (IAM)	IAC-02	Mechanisms exist to facilitate the implementation of Identification and Access Management (IAM) controls.	5		IAC-01			
ISM-2077	Insecure authentication methods	Email is not used for out-of-band authentication purposes.	Functional	Intersects With	Identity & Access Management (IAM)	IAC-02	Mechanisms exist to facilitate the implementation of Identification and Access Management (IAM) controls.	5		IAC-01			
ISM-2078	Password strength	Passwords appearing in lists of commonly used passwords or lists of compromised passwords are not used.	Functional	Intersects With	Automated Support For Password Strength	IAC-15.1	Automated mechanisms exist to determine if password authenticators are sufficiently strong enough to satisfy organization-defined password length and complexity requirements.	5		IAC-10.4			
ISM-2079	Password strength	Maximum length limits for passwords are not less than 64 characters.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-2079	Password strength	Maximum length limits for passwords are not less than 64 characters.	Functional	Intersects With	Password-Based Authentication	IAC-15	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5		IAC-10.1			
ISM-2080	Password strength	Password complexity requirements are not imposed for passwords.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-2080	Password strength	Password complexity requirements are not imposed for passwords.	Functional	Intersects With	Password-Based Authentication	IAC-15	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5		IAC-10.1			
ISM-2081	Password strength	All ASCII printable characters are supported for passwords.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-2081	Password strength	All ASCII printable characters are supported for passwords.	Functional	Intersects With	Password-Based Authentication	IAC-15	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5		IAC-10.1			
ISM-2082	Cryptographic bill of materials	If a cryptographic bill of materials is available for imported third-party software components, it is used during software development to ensure such software components provide support for standardised implementations of ASD-Approved Cryptographic Algorithms.	Functional	Intersects With	Cryptographic Bill of Materials (CBOM)	TDA-21.1	Mechanisms exist to develop and maintain a Cryptographic Bill of Materials (CBOM) by analyzing the organization's cryptographic architecture, including: (1) Hardware; (2) Firmware; (3) Software modules; and (4) Communication protocols.	5		QTS-04.2			
ISM-2083	Cryptographic bill of materials	A cryptographic bill of materials is produced and made available to consumers of software.	Functional	Intersects With	Cryptographic Bill of Materials (CBOM)	TDA-21.1	Mechanisms exist to develop and maintain a Cryptographic Bill of Materials (CBOM) by analyzing the organization's cryptographic architecture, including: (1) Hardware; (2) Firmware; (3) Software modules; and (4) Communication protocols.	5		QTS-04.2			
ISM-2084	Secure artificial intelligence application development	AI-specific documentation, including AI model cards and AI system cards (or equivalent artefacts), is used to document AI model characteristics, system architectures, use cases and security risks.	Functional	Intersects With	AI & Autonomous Technologies Context Definition	AAT-04	Mechanisms exist to establish and document the context surrounding Artificial Intelligence (AI) and Autonomous Technologies (AAT), including: (1) Intended purposes; (2) Potentially beneficial uses; (3) Context-specific laws and regulations; (4) Norms and expectations; and (5) Prospective settings in which the system(s) will be deployed.	5		AAT-03			
ISM-2085	Secure artificial intelligence application development	The exposure of exact AI model confidence scores in API outputs or user interfaces is prevented.	Functional	No Relationship	N/A	N/A	N/A	0					
ISM-2086	Artificial intelligence model poisoning	The source and integrity of AI models, structures and weights are verified.	Functional	Intersects With	Data Source Identification	AAT-18.1	Mechanisms exist to identify and document data sources utilized in the training and/or operation of Artificial Intelligence and Autonomous Technologies (AAT).	5		AAT-12.1			
ISM-2087	Artificial intelligence model poisoning	The source and integrity of training data for AI models is verified.	Functional	Intersects With	Data Source Identification	AAT-18.1	Mechanisms exist to identify and document data sources utilized in the training and/or operation of Artificial Intelligence and Autonomous Technologies (AAT).	5		AAT-12.1			
ISM-2088	Artificial intelligence model poisoning	Data validation and verification techniques are used to ensure the reliability and accuracy of training data used by AI models.	Functional	Intersects With	Training Data Source & Integrity	AAT-18.5	Mechanisms exist to validate the reliability, accuracy and integrity of training data used by Artificial Intelligence and Autonomous Technologies (AAT).	5		AAT-12.5			
ISM-2089	Unbounded consumption	AI model performance metrics are monitored and anomalies are investigated.	Functional	Intersects With	Anomaly Detection & Human Oversight	AAT-36.11	Mechanisms exist to analyze anomalous Artificial Intelligence (AI) and Autonomous Technologies (AAT) behavior and provide escalation paths for human oversight, including: (1) Real-time review; and (2) Intervention.	5		AAT-16.11			
ISM-2090	Unbounded consumption	Rate limiting is applied to inference queries for AI models.	Functional	Intersects With	AI Agent Resource Limiting	AAT-39.24	Automated mechanisms exist to enforce resource limits for Artificial Intelligence (AI) and Autonomous Technologies (AAT), including: (1) Energy consumption; (2) Processing capacity; and (3) Financial consumption (e.g., allocated budget).	5		AAT-29.24			
ISM-2091	Unbounded consumption	Resource limits are enforced for AI models.	Functional	Intersects With	AI Agent Resource Limiting	AAT-39.24	Automated mechanisms exist to enforce resource limits for Artificial Intelligence (AI) and Autonomous Technologies (AAT), including: (1) Energy consumption; (2) Processing capacity; and (3) Financial consumption (e.g., allocated budget).	5		AAT-29.24			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-2092	Excessive agency	Access control policies are implemented to enforce fine-grained permissions for AI applications.	Functional	Intersects With	AI Agent Limitations	AAT-39.2	Mechanisms exist to implement limitations for AI agents according to: (1) Least privileges, where the AI agent operates with the minimal permissions necessary to perform designated tasks; and (2) Least functionality, where the AI agent is restricted to communicate with the minimal Technology Assets, Applications and/or Services (TAAS) and networks necessary to perform designated tasks.	5		AAT-29.2			
ISM-2092	Excessive agency	Access control policies are implemented to enforce fine-grained permissions for AI applications.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-06	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5		IAC-08			
ISM-2093	Excessive agency	Role-based access controls are implemented for AI applications to restrict access to sensitive data.	Functional	Intersects With	AI Agent Data Access Restrictions	AAT-39.7	Mechanisms exist to restrict AI agent access to sensitive and/or regulated data so that AI agents cannot ingest, generate or act on unauthorized data without proper permissions.	8	Updated 2026.3	AAT-29.7			
ISM-2093	Excessive agency	Role-based access controls are implemented for AI applications to restrict access to sensitive data.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-06	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5		IAC-08			
ISM-2094	Sensitive data exposure and improper output	Content filtering is implemented by AI applications to detect and block sensitive data exposure and improper output.	Functional	Intersects With	AI & Autonomous Technologies Harm Prevention	AAT-19	Mechanisms exist to proactively prevent harm by regularly identifying and tracking existing, unanticipated and emergent Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.	5		AAT-17			
ISM-2095	Privately owned mobile devices and desktop computers	Personnel using privately owned mobile devices or desktop computers to access OFFICIAL: Sensitive or PROTECTED systems or data are disallowed from granting access to unapproved artificial intelligence agents.	Functional	Intersects With	Rules of Behavior	HRS-06.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5		HRS-05.1			
ISM-2095	Privately owned mobile devices and desktop computers	Personnel using privately owned mobile devices or desktop computers to access OFFICIAL: Sensitive or PROTECTED systems or data are disallowed from granting access to unapproved artificial intelligence agents.	Functional	Intersects With	Technology Use Restrictions	HRS-06.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	5		HRS-05.3			
ISM-2095	Privately owned mobile devices and desktop computers	Personnel using privately owned mobile devices or desktop computers to access OFFICIAL: Sensitive or PROTECTED systems or data are disallowed from granting access to unapproved artificial intelligence agents.	Functional	Intersects With	Use of Critical Technologies	HRS-06.4	Mechanisms exist to govern usage policies for critical technologies.	5		HRS-05.4			
ISM-2096	Maintaining mobile device security	Mobile devices are configured to enforce separation between organisational and personal mobile applications and data.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-2097	Maintaining mobile device security	Mobile devices are configured with always on VPN functionality.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-2098	Maintaining mobile device security	Mobile devices are configured to prevent data transfers over Universal Serial Bus connections.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-2099	Connecting mobile devices to connected vehicles	Mobile devices are not connected to the infotainment systems of connected vehicles.	Functional	Intersects With	Technology Use Restrictions	HRS-06.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	5		HRS-05.3			
ISM-2100	Using mobile devices within or near connected vehicles	Sensitive or classified data is not viewed on mobile devices within or near connected vehicles.	Functional	Intersects With	Technology Use Restrictions	HRS-06.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	5		HRS-05.3			
ISM-2101	Using mobile devices within or near connected vehicles	Sensitive or classified phone calls and conversations are not conducted within or near connected vehicles.	Functional	Intersects With	Technology Use Restrictions	HRS-06.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	5		HRS-05.3			
ISM-2102	Software artefacts	Existing software artefacts in the authoritative source for software are periodically tested to detect known weaknesses using SAST, DAST or SCA, depending on the software artefact type, throughout the software development life cycle.	Functional	Intersects With	Software Assurance Maturity Model (SAMM)	TDA-03.1	Mechanisms exist to utilize a Software Assurance Maturity Model (SAMM) to govern a secure development lifecycle for the development of Technology Assets, Applications and/or Services (TAAS).	5		TDA-06.3			
ISM-2103	Data collection, retention and use	Organisational data generated, collected or processed by AI applications is not used for training, fine-tuning or improving AI models unless informed and explicit consent has been obtained from data owners in advance.	Functional	Intersects With	Prohibit Training	AAT-18.6	Mechanisms exist to prohibit Artificial Intelligence and Autonomous Technologies (AAT) from training, fine-tuning and/or improving capabilities using organizational data without prior, explicit consent from applicable data owner(s).	5		AAT-12.6			
ISM-2104	Posting work-related information on online services	Personnel are advised not to post information about their security clearance and briefings on unauthorised online services, and to report cases where such information is posted.	Functional	Intersects With	Rules of Behavior	HRS-06.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5		HRS-05.1			
ISM-2104	Posting work-related information on online services	Personnel are advised not to post information about their security clearance and briefings on unauthorised online services, and to report cases where such information is posted.	Functional	Intersects With	Social Media & Social Networking Restrictions	HRS-06.2	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.	5		HRS-05.2			
ISM-2105	Posting work-related information on online services	Personnel are advised to limit posting information about their work-related duties on unauthorised online services, and to report cases where such information is posted.	Functional	Intersects With	Rules of Behavior	HRS-06.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5		HRS-05.1			
ISM-2105	Posting work-related information on online services	Personnel are advised to limit posting information about their work-related duties on unauthorised online services, and to report cases where such information is posted.	Functional	Intersects With	Social Media & Social Networking Restrictions	HRS-06.2	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.	5		HRS-05.2			
ISM-2106	Posting work-related information on online services	Personnel are advised to limit posting information about their work-related skills and experience on unauthorised online services, and to report cases where such information is posted.	Functional	Intersects With	Rules of Behavior	HRS-06.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5		HRS-05.1			
ISM-2106	Posting work-related information on online services	Personnel are advised to limit posting information about their work-related skills and experience on unauthorised online services, and to report cases where such information is posted.	Functional	Intersects With	Social Media & Social Networking Restrictions	HRS-06.2	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.	5		HRS-05.2			
ISM-2107	Posting personal information on online services	Personnel are encouraged to use any available privacy settings to restrict who can view personal information they post on online services.	Functional	Intersects With	Social Media & Social Networking Restrictions	HRS-06.2	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.	5		HRS-05.2			
ISM-2108	Encrypted communications	Mobile applications encrypt all sensitive or classified data communicated over public network infrastructure using ASD-approved cryptography.	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03			
ISM-2109	Encrypting media	Pre-boot authentication using passwords, or managed network-based key release, is implemented for media containing encrypted system volumes.	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	3		CRY-09			
ISM-2109	Encrypting media	Pre-boot authentication using passwords, or managed network-based key release, is implemented for media containing encrypted system volumes.	Functional	Intersects With	Secure Log-On Procedures (Trusted Path)	SEA-27	Mechanisms exist to utilize a trusted communications path between the user and the security functions of the operating system.	3		SEA-17			
ISM-2110	Hardening user application configurations	User applications are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02			
ISM-2111	Hardening user application configurations	All temporary installation files created during user application installation processes are removed after user applications have been installed.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	3	Updated 2026.3	CFG-02			
ISM-2112	Artificial intelligence applications	AI applications that process classified data have their ability to directly access external public data sources disabled.	Functional	Intersects With	AI Agent Limitations	AAT-39.2	Mechanisms exist to implement limitations for AI agents according to: (1) Least privileges, where the AI agent operates with the minimal permissions necessary to perform designated tasks; and (2) Least functionality, where the AI agent is restricted to communicate with the minimal Technology Assets, Applications and/or Services (TAAS) and networks necessary to perform designated tasks.	5	Updated 2026.3	AAT-29.2			
ISM-2113	Artificial intelligence applications	AI applications are configured to flag organisationally defined risky actions for human approval prior to their execution.	Functional	Intersects With	Human-in-the-Loop & Escalation	AAT-36.12	Mechanisms exist to require human review and clear escalation paths for approval for high-risk or ambiguous Artificial Intelligence (AI) and Autonomous Technologies (AAT) actions.	8		AAT-16.12			
ISM-2114	Artificial intelligence applications	Baselines of expected behaviour and performance for AI applications are established and monitored for unexpected deviations.	Functional	Intersects With	AI & Autonomous Technologies Production Monitoring	AAT-36	Mechanisms exist to monitor the functionality and behavior of the deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5		AAT-16			

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Australia - Information Security Manual (ISM) (June 2026)**
Focal Document URL: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-ism-2026-june.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #	Essential 8 ML1	Essential 8 ML2	Essential 8 ML3
ISM-2114	Artificial intelligence applications	Baselines of expected behaviour and performance for AI applications are established and monitored for unexpected deviations.	Functional	Intersects With	AI Agent Behavioral Drift Detection	AAT-39.18	Mechanisms exist to continuously monitor for behavioral drift or deviation from established AI agent baselines.	5		AAT-29.18			
ISM-2115	Hardening server application configurations	Extensions for server applications are restricted to an organisation-approved set.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-14.1	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5		CFG-03.3			
ISM-2116	Event log monitoring	Cyber threat intelligence services are used to support the detection of cyber security events and the identification of cyber security incidents.	Functional	Intersects With	Threat Intelligence Program	THR-02	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	5		THR-01			
ISM-2116	Event log monitoring	Cyber threat intelligence services are used to support the detection of cyber security events and the identification of cyber security incidents.	Functional	Intersects With	Threat Intelligence Feeds	THR-04	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5		THR-03			
ISM-2117	Event log monitoring	Suitable AI models are used to augment the detection of cyber security events and the identification of cyber security incidents.	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	3	Updated 2026.3	MON-01			
ISM-2118	Vulnerability assessments and penetration tests	Vulnerability assessments and penetration tests are conducted for systems prior to their deployment, including prior to the deployment of significant changes, and at least annually thereafter.	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5		VPM-06			
ISM-2118	Vulnerability assessments and penetration tests	Vulnerability assessments and penetration tests are conducted for systems prior to their deployment, including prior to the deployment of significant changes, and at least annually thereafter.	Functional	Intersects With	Penetration Testing	VPM-18	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5		VPM-07			
ISM-2119	Vulnerability assessments and penetration tests	Suitable AI models are used to augment vulnerability assessments and penetration tests.	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	3	Updated 2026.3	VPM-06			
ISM-2119	Vulnerability assessments and penetration tests	Suitable AI models are used to augment vulnerability assessments and penetration tests.	Functional	Intersects With	Penetration Testing	VPM-18	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	3		VPM-07			
ISM-2120	Secure software development	A secure software development policy is developed, implemented and maintained.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10		GOV-02			
ISM-2120	Secure software development	A secure software development policy is developed, implemented and maintained.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-05	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	8		TDA-06			
ISM-2121	Secure software development	Software developers that lack sufficient cyber security knowledge and skills required for their projects or tasks are not used.	Functional	Intersects With	Developer Screening	TDA-19	Mechanisms exist to ensure that the developers of Technology Assets, Applications and/or Services (TAAS) have the requisite skillset and appropriate access authorizations.	5		TDA-13			
ISM-2122	Software security testing	Suitable AI models are used to augment software security testing.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-17	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience 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 control testing and evaluation process; and (3) Document the results.	3	Updated 2026.3	TDA-09			
ISM-2123	Data collection, retention and use	All prompts and outputs associated with chat sessions are securely deleted when chat sessions are removed from AI applications.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	3	Updated 2026.3	CFG-02			