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 - Cloud Controls Matrix (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-cloud-controls-matrix-2026.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 #
GOV-01	Executive cyber security accountability	The board of directors or executive committee is accountable for cyber security.	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
GOV-01	Executive cyber security accountability	The board of directors or executive committee is accountable for cyber security.	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
GOV-08	Executive artificial intelligence accountability	The board of directors or executive committee is accountable for ensuring that artificial intelligence is secure, controllable, human-supervised and used in an ethical and accountable manner.	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
GOV-08	Executive artificial intelligence accountability	The board of directors or executive committee is accountable for ensuring that artificial intelligence is secure, controllable, human-supervised and used in an ethical and accountable manner.	Functional	Intersects With	AI & Autonomous Technologies Human Oversight	AAT-35.1	Mechanisms exist to assign human oversight of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to prevent or minimize the risks to: (1) Health; (2) Safety; and/or	5		AAT-22.1
GOV-08	Executive artificial intelligence accountability	The board of directors or executive committee is accountable for ensuring that artificial intelligence is secure, controllable, human-supervised and used in an ethical and accountable manner.	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
GOV-02	Cyber security leadership	A chief information security officer provides leadership and oversight of cyber security activities and delivers regular and timely risk-based reporting to the board of directors or executive committee on their organisation's cyber security posture, the effectiveness of controls, current security risks and emerging cyber threats.	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
GOV-02	Cyber security leadership	A chief information security officer provides leadership and oversight of cyber security activities and delivers regular and timely risk-based reporting to the board of directors or executive committee on their organisation's cyber security posture, the effectiveness of controls, current security risks and emerging cyber threats.	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
GOV-02	Cyber security leadership	A chief information security officer provides leadership and oversight of cyber security activities and delivers regular and timely risk-based reporting to the board of directors or executive committee on their organisation's cyber security posture, the effectiveness of controls, current security risks and emerging cyber threats.	Functional	Intersects With	Executive Leadership Oversight of Security, Compliance & Resilience Controls	CPL-07	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5		CPL-02
GOV-04	Cyber security resourcing	Suitable and sufficient personnel and resources are identified, acquired and maintained in support of cyber security activities.	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
GOV-04	Cyber security resourcing	Suitable and sufficient personnel and resources are identified, acquired and maintained in support of cyber security activities.	Functional	Intersects With	Position Categorization	HRS-03	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	5		HRS-02
GOV-04	Cyber security resourcing	Suitable and sufficient personnel and resources are identified, acquired and maintained in support of cyber security activities.	Functional	Intersects With	Competency Requirements for Security, Compliance & Resilience-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security, compliance and resilience-related positions are staffed by qualified individuals who have the necessary skill set.	5		HRS-03.2
GOV-04	Cyber security resourcing	Suitable and sufficient personnel and resources are identified, acquired and maintained in support of cyber security activities.	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
GOV-09	Security risk management responsibilities	Security risk management responsibilities for an organisation and their suppliers, partners and customers, including any shared responsibilities, are documented and communicated to all relevant parties with accountability arrangements in place to ensure their effective implementation.	Functional	Intersects With	Customer Responsibility Matrix (CRM)	CLD-03.1	Mechanisms exist to formally document a Customer Responsibility Matrix (CRM), delineating assigned responsibilities for security, compliance and resilience controls between the Cloud Service Provider (CSP) and its customers.	8		CLD-06.1
GOV-09	Security risk management responsibilities	Security risk management responsibilities for an organisation and their suppliers, partners and customers, including any shared responsibilities, are documented and communicated to all relevant parties with accountability arrangements in place to ensure their effective implementation.	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).	8		TPM-05
GOV-03	Security risk management assurance	Security risk management activities for an organisation and their systems (infrastructure, operating systems, applications and data) are embedded into organisational risk management frameworks and subject to ongoing monitoring and assurance activities by the board of directors or executive committee.	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).	3		GOV-01.2
GOV-03	Security risk management assurance	Security risk management activities for an organisation and their systems (infrastructure, operating systems, applications and data) are embedded into organisational risk management frameworks and subject to ongoing monitoring and assurance activities by the board of directors or executive committee.	Functional	Intersects With	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.	8		RSK-01
GOV-05	Security risk acceptance	Residual security risks for systems (infrastructure, operating systems, applications and data), including inherited and shared security risks, are accepted before they are authorised for use and continuously monitored and managed throughout their operational life.	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
GOV-05	Security risk acceptance	Residual security risks for systems (infrastructure, operating systems, applications and data), including inherited and shared security risks, are accepted before they are authorised for use and continuously monitored and managed throughout their operational life.	Functional	Intersects With	Risk Treatment Options	RSK-16.1	Mechanisms exist to select appropriate risk treatment options, based on applicable risk assessment findings, including: (1) Mitigating the risk to an acceptable level; (2) Avoiding the risk (e.g., terminating the project); (3) Transferring the risk to a third party (e.g., insurance and service provider); or (4) Accepting the risk.	5		RSK-06.3
GOV-06	Security risk communication	Residual security risks for systems (infrastructure, operating systems, applications and data), including inherited and shared security risks, are transparently and mutually communicated with stakeholders.	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
GOV-06	Security risk communication	Residual security risks for systems (infrastructure, operating systems, applications and data), including inherited and shared security risks, are transparently and mutually communicated with stakeholders.	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

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 - Cloud Controls Matrix (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-cloud-controls-matrix-2026.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 #
GOV-06	Security risk communication	Residual security risks for systems (infrastructure, operating systems, applications and data), including inherited and shared security risks, are transparently and mutually communicated with stakeholders.	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
GOV-06	Security risk communication	Residual security risks for systems (infrastructure, operating systems, applications and data), including inherited and shared security risks, are transparently and mutually communicated with stakeholders.	Functional	Intersects With	Risk Register	RSK-14	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5		RSK-04.1
GOV-10	System exposure minimisation	Information about the design, configuration and operation of systems (infrastructure, operating systems, applications and data) is not publicly disclosed or shared externally unless necessary for commercial, legal, regulatory or security purposes, with any disclosure minimised, controlled and logged.	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
GOV-10	System exposure minimisation	Information about the design, configuration and operation of systems (infrastructure, operating systems, applications and data) is not publicly disclosed or shared externally unless necessary for commercial, legal, regulatory or security purposes, with any disclosure minimised, controlled and logged.	Functional	Intersects With	Restrict Sensitive / Regulated Data Access To Authorized Individuals	DCH-07.1	Mechanisms exist to control and restrict access to sensitive and/or regulated data on digital and non-digital media formats to authorized individuals.	5		DCH-03
GOV-10	System exposure minimisation	Information about the design, configuration and operation of systems (infrastructure, operating systems, applications and data) is not publicly disclosed or shared externally unless necessary for commercial, legal, regulatory or security purposes, with any disclosure minimised, controlled and logged.	Functional	Intersects With	Publicly Accessible Content	DCH-24	Mechanisms exist to control publicly-accessible content.	5		DCH-15
GOV-10	System exposure minimisation	Information about the design, configuration and operation of systems (infrastructure, operating systems, applications and data) is not publicly disclosed or shared externally unless necessary for commercial, legal, regulatory or security purposes, with any disclosure minimised, controlled and logged.	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
GOV-11	Supplier cyber security assurance	Systems (infrastructure, operating systems, applications and data) are delivered and supported by trustworthy suppliers whose cyber security practices are regularly independently verified or otherwise risk-assessed.	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.	8		TPM-03
GOV-11	Supplier cyber security assurance	Systems (infrastructure, operating systems, applications and data) are delivered and supported by trustworthy suppliers whose cyber security practices are regularly independently verified or otherwise risk-assessed.	Functional	Intersects With	Third-Party Attestation (3PA)	TPM-23	Mechanisms exist to obtain an attestation from an independent Third-Party Assessment Organization (3PAO) that provides assurance of conformity with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to contractors and subcontractors.	5		TPM-05.8
GOV-12	Personnel suitability assurance	Only personnel whose suitability and trustworthiness have been established, and are subject to ongoing assurance, are granted access to systems (infrastructure, operating systems, applications and data).	Functional	Intersects With	Human Resources Security Management	HRS-02	Mechanisms exist to facilitate the implementation of personnel security controls.	5		HRS-01
GOV-12	Personnel suitability assurance	Only personnel whose suitability and trustworthiness have been established, and are subject to ongoing assurance, are granted access to systems (infrastructure, operating systems, applications and data).	Functional	Intersects With	Personnel Screening	HRS-05	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	8		HRS-04
GOV-13	Cyber security and safety	Controls for systems (infrastructure, operating systems, applications and data) do not compromise human, physical or environmental safety.	Functional	Intersects With	Safety Assessment	EMB-19	Mechanisms exist to evaluate the safety aspects of embedded technologies via a fault tree analysis, or similar method, to determine possible consequences of misuse, misconfiguration and/or failure.	3		EMB-15
GOV-14	Legacy system management	Systems (infrastructure, operating systems, applications and data) that are not capable of meeting cyber security requirements are managed using compensating controls, along with enhanced monitoring and assurance activities, to maintain an acceptable level of residual risk until they can be decommissioned or 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
GOV-14	Legacy system management	Systems (infrastructure, operating systems, applications and data) that are not capable of meeting cyber security requirements are managed using compensating controls, along with enhanced monitoring and assurance activities, to maintain an acceptable level of residual risk until they can be decommissioned 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.	8		RSK-06.2
GOV-07	Continuous cyber security improvement	Security risk management and associated cyber security activities are continually measured and reviewed using cyber threat intelligence and assurance activities, including exercises informed by real-world cyber threats, to identify, prioritise and incorporate improvements in governance arrangements, shared responsibilities and the effectiveness of controls.	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
GOV-07	Continuous cyber security improvement	Security risk management and associated cyber security activities are continually measured and reviewed using cyber threat intelligence and assurance activities, including exercises informed by real-world cyber threats, to identify, prioritise and incorporate improvements in governance arrangements, shared responsibilities and the effectiveness of controls.	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
GOV-07	Continuous cyber security improvement	Security risk management and associated cyber security activities are continually measured and reviewed using cyber threat intelligence and assurance activities, including exercises informed by real-world cyber threats, to identify, prioritise and incorporate improvements in governance arrangements, shared responsibilities and the effectiveness of controls.	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.	8		THR-01
GOV-07	Continuous cyber security improvement	Security risk management and associated cyber security activities are continually measured and reviewed using cyber threat intelligence and assurance activities, including exercises informed by real-world cyber threats, to identify, prioritise and incorporate improvements in governance arrangements, shared responsibilities and the effectiveness of controls.	Functional	Intersects With	Predictive Cyber Analytics	THR-10	Mechanisms exist to employ advanced automation and analytics capabilities to predict and identify risks to Technology Assets, Applications, Services and/or Data (TAASD).	5		THR-01.2
IDE-01	Asset identification	Systems (infrastructure, operating systems, applications, identities, credentials and data) are continually and centrally identified and documented.	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.	8		AST-02
IDE-01	Asset identification	Systems (infrastructure, operating systems, applications, identities, credentials and data) are continually and centrally identified and documented.	Functional	Intersects With	Comprehensive Asset Inventory Management	AST-08	Mechanisms exist to maintain a dynamically updated inventory of Technology Assets, Applications, Services and/or Data (TAASD) that provides a highly contextualized understanding of every asset that is capable of providing operational visibility required to: (1) Detect anomalies; (2) Manage complex vulnerabilities; (3) Maintain compliance; and (4) Maintain resilient capabilities.	5		
IDE-05	Asset interdependencies	Interdependencies between systems (infrastructure, operating systems, applications and data) are continually and centrally identified and documented, including how the compromise of one system could affect the security or business operations of other dependent systems.	Functional	Intersects With	Asset-Service Dependencies	AST-06	Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS) that support more than one critical business function.	8		AST-01.1
IDE-02	Business criticality rating identification	Business criticality ratings for systems (infrastructure, operating systems, applications and data) are identified and documented.	Functional	Equal	Technology Assets, Applications, Services and/or Data (TAASD) Criticality Ratings	AST-05.1	Mechanisms exist to assign Business Continuity & Disaster Recovery (BC/DR)-relevant criticality ratings for Technology Assets, Applications, Services and/or Data (TAASD).	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 - Cloud Controls Matrix (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-cloud-controls-matrix-2026.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 #
IDE-03	Security requirement identification	Security requirements for systems (infrastructure, operating systems, applications and data) are identified and documented.	Functional	Subset Of	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).	10		PRM-05
IDE-06	Resilience requirement identification	Resilience requirements for systems (infrastructure, operating systems, applications and data) are identified and documented.	Functional	Subset Of	Defined Operational Resilience Requirements	BCD-02.1	Mechanisms exist to define operational resilience requirements for Technology Assets, Applications, Services and/or Data (TAASD) to operate in a controlled and acceptable manner during: (1) Routine operations; and (2) Adverse conditions.	10		
IDE-06	Resilience requirement identification	Resilience requirements for systems (infrastructure, operating systems, applications and data) are identified and documented.	Functional	Subset Of	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	10		PRM-05
IDE-04	Security risk identification	Security risks for an organisation and their systems (infrastructure, operating systems, applications and data) are identified, including by using current strategic and sector-specific cyber threat intelligence and threat modelling, and are documented along with any associated risk management decisions.	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
IDE-04	Security risk identification	Security risks for an organisation and their systems (infrastructure, operating systems, applications and data) are identified, including by using current strategic and sector-specific cyber threat intelligence and threat modelling, and are documented along with any associated risk management decisions.	Functional	Intersects With	Threat Analysis & Flaw Remediation During Development	IAO-10	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	5		IAO-04
IDE-04	Security risk identification	Security risks for an organisation and their systems (infrastructure, operating systems, applications and data) are identified, including by using current strategic and sector-specific cyber threat intelligence and threat modelling, and are documented along with any associated risk management decisions.	Functional	Intersects With	Risk Treatment Options	RSK-16.1	Mechanisms exist to select appropriate risk treatment options, based on applicable risk assessment findings, including: (1) Mitigating the risk to an acceptable level; (2) Avoiding the risk (e.g., terminating the project); (3) Transferring the risk to a third party (e.g., insurance and service provider); or (4) Accepting the risk.	5		RSK-06.3
IDE-04	Security risk identification	Security risks for an organisation and their systems (infrastructure, operating systems, applications and data) are identified, including by using current strategic and sector-specific cyber threat intelligence and threat modelling, and are documented along with any associated risk management decisions.	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
IDE-04	Security risk identification	Security risks for an organisation and their systems (infrastructure, operating systems, applications and data) are identified, including by using current strategic and sector-specific cyber threat intelligence and threat modelling, and are documented along with any associated risk management decisions.	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
PRO-01	Secure system lifecycle	Systems (infrastructure, operating systems and applications) are planned, designed, developed, tested, deployed, maintained and decommissioned according to their business criticality ratings and security and resilience requirements using Secure by Design and Secure by Default principles and practices.	Functional	Intersects With	Security, Compliance & Resilience Aware Design	SEA-02	Mechanisms exist to formally incorporate the organization's secure architecture principles into engineering, product and model design requirements to ensure security, compliance and resilience are built in by default and by design.	8		SEA-01.5
PRO-01	Secure system lifecycle	Systems (infrastructure, operating systems and applications) are planned, designed, developed, tested, deployed, maintained and decommissioned according to their business criticality ratings and security and resilience requirements using Secure by Design and Secure by Default principles and practices.	Functional	Intersects With	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.	8		TDA-01
PRO-16	Cyber supply chain security	Cyber supply chains supporting systems (infrastructure, operating systems, applications and data) are secure, resilient and support effective and coordinated cyber security incident response.	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.	3		IRO-10.4
PRO-16	Cyber supply chain security	Cyber supply chains supporting systems (infrastructure, operating systems, applications and data) are secure, resilient and support effective and coordinated cyber security incident response.	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.	8		RSK-09
PRO-16	Cyber supply chain security	Cyber supply chains supporting systems (infrastructure, operating systems, applications and data) are secure, resilient and support effective and coordinated cyber security incident response.	Functional	Subset Of	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.	10		TPM-03
PRO-13	Identity, credential and access management	Robust and secure identity, credential and access management is used to establish, maintain and control access to systems (infrastructure, operating systems, applications and data) and to support effective detection of identity and credential misuse.	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
PRO-13	Identity, credential and access management	Robust and secure identity, credential and access management is used to establish, maintain and control access to systems (infrastructure, operating systems, applications and data) and to support effective detection of identity and credential misuse.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	3		MON-16
PRO-12	Least privilege access	Personnel and services are granted the minimum access to systems (infrastructure, operating systems, applications and data) required to undertake their duties.	Functional	Equal	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.	10		IAC-21
PRO-05	Secure administration	Systems (infrastructure, operating systems, applications and data) are administered in a secure, accountable and auditable manner.	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).	8		AST-26
PRO-04	Secure configuration management	Systems (infrastructure, operating systems and applications) are securely configured to approved and maintained baselines, including by reducing attack surfaces and attack paths, with configurations continually monitored and consistently 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.	8		CFG-02
PRO-04	Secure configuration management	Systems (infrastructure, operating systems and applications) are securely configured to approved and maintained baselines, including by reducing attack surfaces and attack paths, with configurations continually monitored and consistently enforced.	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		CFG-06
PRO-06	Vulnerability management	Vulnerabilities in systems (infrastructure, operating systems, applications and data) are identified, documented, validated and prioritised for remediation or mitigation in a timely manner, with all remediation and mitigation actions verified for effectiveness.	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
PRO-06	Vulnerability management	Vulnerabilities in systems (infrastructure, operating systems, applications and data) are identified, documented, validated and prioritised for remediation or mitigation in a timely manner, with all remediation and mitigation actions verified for effectiveness.	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.	3		VPM-03
PRO-06	Vulnerability management	Vulnerabilities in systems (infrastructure, operating systems, applications and data) are identified, documented, validated and prioritised for remediation or mitigation in a timely manner, with all remediation and mitigation actions verified for effectiveness.	Functional	Intersects With	Vulnerability Remediation Process	VPM-06	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	8		VPM-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 - Cloud Controls Matrix (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-cloud-controls-matrix-2026.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 #
PRO-07	Trustworthy software	Systems (operating systems and applications) only permit the execution of software that is supported, verified and authorised.	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
PRO-07	Trustworthy software	Systems (operating systems and applications) only permit the execution of software that is supported, verified and authorised.	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.	8		CFG-03.3
PRO-08	Cryptographic protection	Data is encrypted and authenticated at rest and in transit using ASD-approved cryptography to protect its confidentiality and integrity.	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.	8		CRY-01
PRO-08	Cryptographic protection	Data is encrypted and authenticated at rest and in transit using ASD-approved cryptography to protect its confidentiality and integrity.	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03
PRO-08	Cryptographic protection	Data is encrypted and authenticated at rest and in transit using ASD-approved cryptography to protect its confidentiality and integrity.	Functional	Intersects With	Integrity of Data In Transit	CRY-06	Cryptographic mechanisms exist to detect unauthorized changes to data in transit.	5		CRY-04
PRO-08	Cryptographic protection	Data is encrypted and authenticated at rest and in transit using ASD-approved cryptography to protect its confidentiality and integrity.	Functional	Intersects With	Encrypting Data At Rest	CRY-07	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data at rest.	5		CRY-05
PRO-17	Cryptographic agility	Systems (infrastructure, operating systems and applications) are designed, configured and managed to support timely, prioritised and orderly changes to cryptography, including post-quantum 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
PRO-17	Cryptographic agility	Systems (infrastructure, operating systems and applications) are designed, configured and managed to support timely, prioritised and orderly changes to cryptography, including post-quantum cryptography.	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.	5		QTS-03
PRO-10	Regular and proven backups	Systems (infrastructure, operating systems, applications and data) are regularly backed up in a secure and proven manner, including through the validation of restoration capabilities.	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
PRO-10	Regular and proven backups	Systems (infrastructure, operating systems, applications and data) are regularly backed up in a secure and proven manner, including through the validation of restoration capabilities.	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
PRO-18	Network segmentation and segregation	Systems (infrastructure, operating systems and applications) are segmented into network zones based on business criticality and trust levels, with only authorised, controlled and monitored inbound and outbound communication paths between network zones permitted.	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
PRO-18	Network segmentation and segregation	Systems (infrastructure, operating systems and applications) are segmented into network zones based on business criticality and trust levels, with only authorised, controlled and monitored inbound and outbound communication paths between network zones permitted.	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
PRO-19	Operational technology isolation	Operational technology systems (infrastructure) are logically and physically isolated from information technology systems (infrastructure) and all external infrastructure, with only authorised, controlled and monitored communication paths between systems permitted.	Functional	Intersects With	Separate Operating Environments For Embedded Technologies	EMB-03	Mechanisms exist to logically or physically separate embedded technologies from organizational Information Technology (IT) networks.	8		
PRO-19	Operational technology isolation	Operational technology systems (infrastructure) are logically and physically isolated from information technology systems (infrastructure) and all external infrastructure, with only authorised, controlled and monitored communication paths between systems permitted.	Functional	Intersects With	Operational Technology (OT)	EMB-06	Mechanisms exist to proactively manage the security, compliance and resilience risks associated with Operational Technology (OT).	5		EMB-03
PRO-19	Operational technology isolation	Operational technology systems (infrastructure) are logically and physically isolated from information technology systems (infrastructure) and all external infrastructure, with only authorised, controlled and monitored communication paths between systems permitted.	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
PRO-20	Remote access to operational technology	Access to operational technology systems (infrastructure, operating systems, applications and data) over untrusted infrastructure is authorised, controlled and monitored.	Functional	Intersects With	Separate Operating Environments For Embedded Technologies	EMB-03	Mechanisms exist to logically or physically separate embedded technologies from organizational Information Technology (IT) networks.	5		
PRO-20	Remote access to operational technology	Access to operational technology systems (infrastructure, operating systems, applications and data) over untrusted infrastructure is authorised, controlled and monitored.	Functional	Intersects With	Remote Management of Embedded Technologies	EMB-15	Mechanisms exist to restrict remote management of embedded technologies by: (1) Allowing access only when needed; (2) Eliminating "always on" connections; and (3) Requiring strong authentication.	5		
PRO-09	Content filtering	Data communicated between different security domains for systems (infrastructure and applications) is controlled and subject to inspection and verification.	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
PRO-09	Content filtering	Data communicated between different security domains for systems (infrastructure and applications) is controlled and subject to inspection and verification.	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
PRO-14	Cyber security awareness training	Personnel are provided with ongoing cyber security awareness training, including operational security considerations, tailored to their duties, access levels and current cyber threats.	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
PRO-14	Cyber security awareness training	Personnel are provided with ongoing cyber security awareness training, including operational security considerations, tailored to their duties, access levels and current cyber threats.	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
PRO-14	Cyber security awareness training	Personnel are provided with ongoing cyber security awareness training, including operational security considerations, tailored to their duties, access levels and current cyber threats.	Functional	Intersects With	Cyber Threat Environment Situational Awareness	SAT-06	Mechanisms exist to provide role-based security, compliance and resilience awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5		SAT-03.6
PRO-15	Physical access control	Physical access to facilities and systems (infrastructure and data) is restricted to authorised personnel and monitored for unusual activities.	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
PRO-15	Physical access control	Physical access to facilities and systems (infrastructure and data) is restricted to authorised personnel and monitored for unusual activities.	Functional	Intersects With	Monitoring Physical Access	PES-13	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	5		PES-05
DET-01	Centralised event logging	Security-relevant event logs and configuration changes for systems (infrastructure, operating systems, applications and data) are centrally collected, protected against unauthorised modification or deletion, and retained to support effective cyber security event detection and investigation.	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
DET-01	Centralised event logging	Security-relevant event logs and configuration changes for systems (infrastructure, operating systems, applications and data) are centrally collected, protected against unauthorised modification or deletion, and retained to support effective cyber security event detection and investigation.	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.	5		MON-08
DET-01	Centralised event logging	Security-relevant event logs and configuration changes for systems (infrastructure, operating systems, applications and data) are centrally collected, protected against unauthorised modification or deletion, and retained to support effective cyber security event detection and investigation.	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
DET-04	Baselined high-risk access activities	Baseline patterns of identity and credential access activities, privileged access activities, and remote access activities are established and maintained for systems (infrastructure, operating systems, applications and data) to enable the detection of anomalous or unexpected behaviour.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5		MON-16
DET-04	Baselined high-risk access activities	Baseline patterns of identity and credential access activities, privileged access activities, and remote access activities are established and maintained for systems (infrastructure, operating systems, applications and data) to enable the detection of anomalous or unexpected behaviour.	Functional	Intersects With	Behavioral Baselining	THR-09	Automated mechanisms exist to establish behavioral baselines that capture information about user and entity behavior to enable dynamic threat discovery.	5		THR-11
DET-02	Cyber security event detection	Anomalous or unexpected events and behaviours for systems (infrastructure, operating systems, applications and data) are analysed in a timely manner to detect cyber security events.	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

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 - Cloud Controls Matrix (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-cloud-controls-matrix-2026.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 #
DET-02	Cyber security event detection	Anomalous or unexpected events and behaviours for systems (infrastructure, operating systems, applications and data) are analysed in a timely manner to detect cyber security events.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5		MON-16
DET-03	Cyber security incident identification	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
DET-03	Cyber security incident identification	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
DET-03	Cyber security incident identification	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
DET-05	Detection capability efficacy	Cyber security event detection capabilities are regularly evaluated for effectiveness and continuously refined, including by using current strategic and sector-specific cyber threat intelligence, to improve the detection of cyber security events.	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
DET-05	Detection capability efficacy	Cyber security event detection capabilities are regularly evaluated for effectiveness and continuously refined, including by using current strategic and sector-specific cyber threat intelligence, to improve the detection of cyber security events.	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.	3		THR-03
RES-01	Cyber security incident planning	Cyber security incident response, business continuity and disaster recovery plans for systems (infrastructure, operating systems, applications and data) support continued business operations during cyber security incidents, and the resumption of normal business operations following cyber security incidents.	Functional	Intersects With	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.	5		BCD-01
RES-01	Cyber security incident planning	Cyber security incident response, business continuity and disaster recovery plans for systems (infrastructure, operating systems, applications and data) support continued business operations during cyber security incidents, and the resumption of normal business operations following cyber security incidents.	Functional	Intersects With	Business Continuity & Disaster Recovery (BC/DR) Plans	BCD-04	Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.	5		BCD-01.7
RES-01	Cyber security incident planning	Cyber security incident response, business continuity and disaster recovery plans for systems (infrastructure, operating systems, applications and data) support continued business operations during cyber security incidents, and the resumption of normal business operations following cyber security incidents.	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
RES-05	Cyber security incident coordination	Cyber security incident roles and responsibilities are defined, documented and exercised to support the internal and external coordination and management of cyber security incidents, including responsibilities for declaring cyber security incidents and undertaking pre-approved response and recovery activities.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-04	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5		HRS-03
RES-05	Cyber security incident coordination	Cyber security incident roles and responsibilities are defined, documented and exercised to support the internal and external coordination and management of cyber security incidents, including responsibilities for declaring cyber security incidents and undertaking pre-approved response and recovery activities.	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
RES-03	Cyber security incident response	Cyber security incidents are contained, eradicated and recovered from in a timely manner.	Functional	Subset Of	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.	10		IRO-02
RES-02	Cyber security incident reporting	Cyber security incidents, including associated response and recovery activities, are reported internally and externally to relevant bodies and stakeholders in a timely manner.	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
RES-04	Cyber security incident insights	Lessons learnt from cyber security incidents are captured, and areas for improvement are identified, prioritised and actioned in a timely manner.	Functional	Subset Of	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.	10		IRO-13
REC-02	System recovery assurance	Following cyber security incidents, systems (infrastructure, operating systems, applications and data) are verified through assurance activities to ensure they are secure and capable of supporting the resumption of normal business operations.	Functional	Subset Of	Post-Incident Technology Assets, Applications and Services (TAAS) Validation	IRO-26	Mechanisms exist to utilize post-incident assurance activities to validate Technology Assets, Applications and Services (TAAS) are (1) Secure; (2) Compliant; and (3) Capable of supporting the resumption of normal business operations.	10		
REC-01	Business operations resumption	Residual security risks for systems (infrastructure, operating systems, applications and data), including inherited and shared security risks, are accepted prior to the resumption of normal business operations following cyber security incidents.	Functional	Intersects With	Post-Incident Technology Assets, Applications and Services (TAAS) Validation	IRO-26	Mechanisms exist to utilize post-incident assurance activities to validate Technology Assets, Applications and Services (TAAS) are (1) Secure; (2) Compliant; and (3) Capable of supporting the resumption of normal business operations.	5		
REC-01	Business operations resumption	Residual security risks for systems (infrastructure, operating systems, applications and data), including inherited and shared security risks, are accepted prior to the resumption of normal business operations following cyber security incidents.	Functional	Subset Of	Risk Treatment Options	RSK-16.1	Mechanisms exist to select appropriate risk treatment options, based on applicable risk assessment findings, including: (1) Mitigating the risk to an acceptable level; (2) Avoiding the risk (e.g., terminating the project);	10		RSK-06.3