NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
1.1.64.C.01	Non-compliance	System owners seeking a dispensation for non-compliance with any baseline controls in the NZISM MUST be granted a dispensation by their Accreditation Authority. Where High Assurance Cryptographic Systems (HACS) are implemented, the Accreditation Authority will be the Director-General GCSB or a formal delegate.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
1.1.65.C.01	Justification for non-compliance	System owners seeking a dispensation for non-compliance with baseline controls MUST complete an agency risk assessment which documents: the reason(s) for not being able to comply with this manual; the effect on any of their own, multi-agency or All-of-Government system; the alternative mitigation measure(s) to be implemented; The strength and applicability of the alternative mitigations; an assessment of the residual security risk(s); and a date by which to review the decision.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
1.1.66.C.01	Consultation on non-compliance	If a system processes, stores or communicates classified information from another agency, that agency MUST be consulted before a decision to be non-compliant with the NZ Government Security Classification System is made.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
1.1.66.C.02	Consultation on non-compliance	If a system processes, stores or communicates classified information from a foreign government, that government MUST be consulted before a decision to be non-compliant with NZISM controls is made.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
1.1.67.C.01	All-of-Government Systems	If a system processes, stores or communicates data and information with multiple agencies or forms part of an All-of-Government system, interested parties MUST be formally consulted before non-compliance with any baseline controls.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
1.1.68.C.01	Reviewing non-compliance	Agencies SHOULD review decisions to be non-compliant with any controls at least annually.	Functional	Intersects With	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	5	
1.1.69.C.01	Recording non-compliance	Agencies MUST retain a copy and maintain a record of the supporting risk assessment and decisions to be non-compliant with any baseline controls from the NZISM.	Functional	Intersects With	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	5	
1.1.69.C.02	Recording non-compliance	Where good and recommended practice controls are NOT implemented, agencies MUST record and formally recognise that non-use of any controls without due consideration may increase residual risk for the agency. This residual risk MUST be agreed and acknowledged by the Accreditation Authority.	Functional	Intersects With	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	5	
1.2.15.C.01	Compliance	Agencies undertaking system design activities for in-house or out-sourced projects MUST use the latest version of the NZISM for information security requirements.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
1.2.15.C.01	Compliance	Agencies undertaking system design activities for in-house or out-sourced projects MUST use the latest version of the NZISM for information security requirements.	Functional	Intersects With	Secure Architecture Principles	SEA-01.4	Mechanisms exist to ensure security, compliance and resilience capabilities are designed and maintained in alignment with security architecture principles from: (1) The Open Group Architecture Framework (TOGAF); (2) Sherwood Applied Business Security Architecture (SABSA); and/or (3) An organization-defined reference architecture.	8	
1.2.15.C.02	Compliance	When GCSB makes a determination that newly introduced standard, policy or guideline within the NZISM, or any additional information security policy, is of particular importance, agencies MUST comply with any new specified requirements and implementation timeframes.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
2.1.47.C.01	Organisations providing information security services	Security personnel MUST familiarise themselves with the information security roles and services provided by New Zealand Government organisations.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	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	
2.2.5.C.01	Outsourcing information technology services and functions	Agencies engaging industry for the provision of off-site information technology services and functions MUST accredit the systems used by the contractor to at least the same minimum standard as the agency's systems. This may be achieved through a third party review report utilising the ISAE 3402 Assurance Reports on Controls at a Third Party Service Organisation.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
2.2.5.C.01	Outsourcing information technology services and functions	Agencies engaging industry for the provision of off-site information technology services and functions MUST accredit the systems used by the contractor to at least the same minimum standard as the agency's systems. This may be achieved through a third party review report utilising the ISAE 3402 Assurance Reports on Controls at a Third Party Service Organisation.	Functional	Intersects With	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	5	
2.2.5.C.02	Outsourcing information technology services and functions	Agencies SHOULD NOT engage industry for the provision of off-site information technology services and functions in countries that New Zealand does not have a multilateral or bilateral security agreement with for the protection of classified information of the government of New Zealand. If there is any doubt, the agency's CISO should be consulted.	Functional	Intersects With	Adequate Security for Sensitive / Regulated Data In Support of Contracts	IAO-03.2	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	
2.2.6.C.01	Independence of ITSMs from outsourced companies	Where an agency has outsourced information technology services and functions, any ITSMs within the agency SHOULD be independent of the company providing the information technology services and functions.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
2.2.6.C.02	Independence of ITSMs from outsourced companies	Where an agency has outsourced information technology services and functions, they SHOULD ensure that the outsourced organisation provides a single point of contact within the organisation for all information assurance and security matters.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
2.2.7.C.01	Developing a contractor management program	Agencies SHOULD develop a program to manage contractors that have been accredited for the provision of off-site information technology services and functions.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
2.3.25.C.01	Cloud Adoption Strategy	Agencies intending to adopt public cloud technologies or services MUST develop a plan for how they intend to use these services. This plan can be standalone or part of an overarching ICT strategy.	Functional	Intersects With	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a: (1) Strategic security, compliance and resilience-specific business plan; and (2) Set of objectives to achieve that plan.	5	
2.3.25.C.02	Cloud Adoption Strategy	An agency's cloud adoption plan SHOULD cover: Outcomes and benefits that the adoption of cloud technologies will bring; Risks introduced or mitigated through the use of cloud, and the agency's risk tolerance; Financial and cost accounting models; Shared responsibility models; Cloud deployment models; Cloud security strategy; Resilience and recovery approaches; Data recovery on contract termination; Cloud exit strategy and other contractual arrangements; and A high level description of the foundation services that enable cloud adoption, including: User, device and system identity; Encryption and key management; Information management; Logging and alerting; Incident management; Managing privileged activities; and Cost management.	Functional	Intersects With	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a: (1) Strategic security, compliance and resilience-specific business plan; and (2) Set of objectives to achieve that plan.	5	
2.3.26.C.01	Zero Trust	Agencies intending to adopt public cloud technologies or services SHOULD incorporate Zero Trust philosophies and concepts.	Functional	Intersects With	Zero Trust Architecture (ZTA)	NET-01.1	Mechanisms exist to treat all users and devices as potential threats and prevent access to data and resources until the users can be properly authenticated and their access authorized.	5	
2.3.26.C.02	Zero Trust	Agencies SHOULD leverage public cloud environment native security services as part of legacy system migrations, in preference to recreating application architectures that rely on legacy perimeter controls for security.	Functional	Intersects With	Zero Trust Architecture (ZTA)	NET-01.1	Mechanisms exist to treat all users and devices as potential threats and prevent access to data and resources until the users can be properly authenticated and their access authorized.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
2.3.27.C.01	Risk Assessment	Agencies intending to adopt cloud technologies or services MUST conduct a comprehensive risk assessment, in accordance with the guidance provided by the Government Chief Digital Officer (GCDO) before implementation or adoption.	Functional	Intersects With	Risk Assessment	RSK-04	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	
2.3.27.C.02	Risk Assessment	Agencies MUST ensure cloud risks for any cloud service adopted are identified, understood and formally accepted by the Agency Head or Chief Executive and the agency's Accreditation Authority.	Functional	Intersects With	Risk Assessment	RSK-04	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	
2.3.28.C.01	Security Architecture	Agencies intending to adopt cloud services SHOULD review and enhance existing security architectures and systems design to prudently manage the changed risk, technology and security environment in adopting cloud services.	Functional	Subset Of	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	10	
2.3.28.C.01	Security Architecture	Agencies intending to adopt cloud services SHOULD review and enhance existing security architectures and systems design to prudently manage the changed risk, technology and security environment in adopting cloud services.	Functional	Intersects With	Cloud Security Architecture	CLD-02	Mechanisms exist to ensure the cloud security architecture supports the organization's technology strategy to securely design, configure and maintain cloud employments.	8	
2.3.28.C.01	Security Architecture	Agencies intending to adopt cloud services SHOULD review and enhance existing security architectures and systems design to prudently manage the changed risk, technology and security environment in adopting cloud services.	Functional	Intersects With	Secure Engineering Principles	SEA-01	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).	8	
2.3.28.C.01	Security Architecture	Agencies intending to adopt cloud services SHOULD review and enhance existing security architectures and systems design to prudently manage the changed risk, technology and security environment in adopting cloud services.	Functional	Intersects With	Secure Architecture Principles	SEA-01.4	Mechanisms exist to ensure security, compliance and resilience capabilities are designed and maintained in alignment with security architecture principles from: (1) The Open Group Architecture Framework (TOGAF); (2) Sherwood Applied Business Security Architecture (SABSA); and/or (3) An organization-defined reference architecture.	8	
2.3.28.C.01	Security Architecture	Agencies intending to adopt cloud services SHOULD review and enhance existing security architectures and systems design to prudently manage the changed risk, technology and security environment in adopting cloud services.	Functional	Intersects With	Security-Aware Design	SEA-01.5	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	
2.3.29.C.01	Selection of Services	Agencies MUST consider the use of any All of Government contracts with cloud service providers before negotiating individual contracts.	Functional	Intersects With	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a: (1) Strategic security, compliance and resilience-specific business plan; and (2) Set of objectives to achieve that plan.	5	
2.3.30.C.01	System Decommissioning and Contract Termination	Agency system architectures and supply arrangements and contracts SHOULD include provision for the safe return of agency data in the event of system or service termination or contract termination.	Functional	Intersects With	Decommissioning	AST-30	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are properly decommissioned so that data is properly transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	
2.3.30.C.01	System Decommissioning and Contract Termination	Agency system architectures and supply arrangements and contracts SHOULD include provision for the safe return of agency data in the event of system or service termination or contract termination.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	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	
2.4.13.C.01	Post-Quantum Cryptography Preparation	Agencies SHOULD ensure they are aware of the latest developments in post-quantum cryptography. GCSB is tracking these developments and will continue to provide advice through the NZISM.	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
2.4.13.C.02	Post-Quantum Cryptography Preparation	Agencies SHOULD maintain an inventory of sensitive and critical datasets that must be secured for an extended amount of time. This will ensure datasets that may be at risk now and decrypted once a cryptographically relevant quantum computer is available are not secured solely through the use of quantum vulnerable cryptography.	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
2.4.13.C.03	Post-Quantum Cryptography Preparation	Agencies SHOULD conduct an inventory of systems using cryptographic technologies to determine the potential size and scope of future transition work once post-quantum cryptographic systems become available.	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
2.4.13.C.04	Post-Quantum Cryptography Preparation	Agencies SHOULD identify which systems in their inventory rely on public key cryptography and note them as quantum vulnerable in agency risk assessments.	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
2.4.13.C.05	Post-Quantum Cryptography Preparation	Agencies SHOULD determine a priority order for quantum vulnerable systems to be transitioned from classical cryptography to post-quantum cryptography.	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
2.4.13.C.06	Post-Quantum Cryptography Preparation	Agencies SHOULD consider the following factors when prioritising the quantum vulnerable systems: Is the system a high value asset based on agency requirements? Does the system protect sensitive information (e.g., key stores, passwords, root keys, signing keys, personal information, and classified information)? Do other systems (internal or external to the agency) depend on the cryptographic protections in place on the quantum vulnerable system? How long does the data need to be protected?	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
2.4.13.C.07	Post-Quantum Cryptography Preparation	Using the inventory and prioritisation information, agencies SHOULD develop a plan for system transitions upon publication of the new post-quantum cryptographic standard.	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
3.1.8.C.01	Delegation of authority	Where the agency head devolves their authority the delegate MUST be at least a member of the Senior Executive Team or an equivalent management position.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
3.1.8.C.02	Delegation of authority	When the agency head delegates their authority, the delegate SHOULD be a senior executive who understands the consequences and potential impact to the business of the acceptance of residual risk.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
3.1.8.C.03	Delegation of authority	Where the head of a smaller agency is not able to satisfy all segregation of duty requirements because of scalability and small personnel numbers, all potential conflicts of interest SHOULD be clearly identified, declared and actively managed.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
3.1.9.C.01	Support for information security	The agency head MUST provide support for the development, implementation and ongoing maintenance of information security processes within their agency.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
3.2.8.C.01	Requirement for a CISO	The CISO MUST be: cleared for access to all classified information processed by the agency's systems, and able to be briefed into any compartmented information on the agency's systems.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
3.2.8.C.02	Requirement for a CISO	Agencies SHOULD appoint a person to the role of CISO or have the role undertaken by an existing person within the agency.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
3.2.8.C.03	Requirement for a CISO	The CISO role SHOULD be undertaken by a member of the Senior Executive Team or an equivalent management position.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
3.2.8.C.04	Requirement for a CISO	The CISO SHOULD be responsible for overseeing the management of security personnel within the agency.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
3.2.8.C.05	Requirement for a CISO	Where multiple roles are held by the CISO any potential conflicts of interest SHOULD be identified and carefully managed.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
3.2.9.C.01	Responsibilities - Reporting	The CISO SHOULD report directly to the agency head on matters of information security within the agency.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	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	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
3.2.9.C.01	Responsibilities - Reporting	The CISO SHOULD report directly to the agency head on matters of information security within the agency.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
3.2.10.C.01	Responsibilities - Security programs	The CISO SHOULD develop and maintain a comprehensive strategic level information security and security risk management program within the agency aimed at protecting the agency's official and classified information.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
3.2.10.C.02	Responsibilities - Security programs	The CISO SHOULD be responsible for the development of an information security communications plan.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
3.2.10.C.03	Responsibilities - Security programs	The CISO SHOULD create and facilitate the agency security risk management process.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
3.2.10.C.04	Responsibilities - Security programs	The CISO SHOULD work with system owners, system certifiers and system accreditors to determine appropriate information security policies for their systems and ensure consistency with the Protective Security Requirements (PSR) and in particular the relevant NZISM components.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
3.2.10.C.04	Responsibilities - Security programs	The CISO SHOULD work with system owners, system certifiers and system accreditors to determine appropriate information security policies for their systems and ensure consistency with the Protective Security Requirements (PSR) and in particular the relevant NZISM components.	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	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	
3.2.10.C.04	Responsibilities - Security programs	The CISO SHOULD work with system owners, system certifiers and system accreditors to determine appropriate information security policies for their systems and ensure consistency with the Protective Security Requirements (PSR) and in particular the relevant NZISM components.	Functional	Intersects With	Select Controls	GOV-15.1	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	
3.2.11.C.01	Responsibilities - Ensuring compliance	The CISO SHOULD be responsible for establishing mechanisms and programs to ensure compliance with the information security policies and standards within the agency.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
3.2.11.C.02	Responsibilities - Ensuring compliance	The CISO SHOULD be responsible for ensuring agency compliance with the NZISM through facilitating a continuous program of certification and accreditation of all agency systems.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
3.2.11.C.03	Responsibilities - Ensuring compliance	The CISO SHOULD be responsible for the implementation of information security measurement metrics and key performance indicators within the agency.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
3.2.12.C.01	Responsibilities - Coordinating security	The CISO SHOULD facilitate information security and business alignment and communication through an information security steering committee or advisory board which meets formally and on a regular basis, and comprises key business and ICT executives.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
3.2.12.C.02	Responsibilities - Coordinating security	The CISO SHOULD be responsible for coordinating information security and security risk management projects between business and information security teams.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
3.2.12.C.03	Responsibilities - Coordinating security	The CISO SHOULD work with business teams to facilitate security risk analysis and security risk management processes, including the identification of acceptable levels of risk consistently across the agency.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
3.2.13.C.01	Responsibilities - Working with ICT projects	The CISO SHOULD provide strategic level guidance for agency ICT projects and operations.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
3.2.13.C.02	Responsibilities - Working with ICT projects	The CISO SHOULD liaise with agency technology architecture teams to ensure alignment between security and agency architectures.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
3.2.14.C.01	Responsibilities - Working with vendors	The CISO SHOULD coordinate the use of external information security resources to the agency including contracting and managing the resources.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
3.2.15.C.01	Responsibilities - Budgeting	The CISO SHOULD be responsible for controlling the information security budget.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
3.2.15.C.01	Responsibilities - Budgeting	The CISO SHOULD be responsible for controlling the information security budget.	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	
3.2.15.C.01	Responsibilities - Budgeting	The CISO SHOULD be responsible for controlling the information security budget.	Functional	Intersects With	Security, Compliance & Resilience Resource Management	PRM-02	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 to this requirement.	5	
3.2.16.C.01	Responsibilities - Information security incidents	The CISO SHOULD be fully aware of all information security incidents within the agency.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
3.2.16.C.01	Responsibilities - Information security incidents	The CISO SHOULD be fully aware of all information security incidents within the agency.	Functional	Intersects With	Situational Awareness For Incidents	IRO-09	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	
3.2.17.C.01	Responsibilities - Disaster recovery	The CISO SHOULD coordinate the development of disaster recovery policies and standards within the agency to ensure that business-critical services are supported appropriately and that information security is maintained in the event of a disaster.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
3.2.18.C.01	Responsibilities - Training	The CISO SHOULD be responsible for overseeing the development and operation of information security awareness and training programs within the agency.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
3.2.19.C.01	Responsibilities - Providing security knowledge	The CISO SHOULD provide authoritative security advice and have familiarity with a range of national and international standards and good practice.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
3.2.19.C.01	Responsibilities - Providing security knowledge	The CISO SHOULD provide authoritative security advice and have familiarity with a range of national and international standards and good practice.	Functional	Intersects With	Manage Organizational Knowledge	PRM-08	Mechanisms exist to manage the organizational knowledge of the security, compliance and resilience staff.	5	
3.3.4.C.01	Requirement for ITSMs	Agencies MUST appoint at least one ITSM within their agency.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.3.4.C.02	Requirement for ITSMs	ITSMs MUST be: cleared for access to all classified information processed by the agency's systems; and able to be briefed into any compartmented information on the agency's systems.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.3.4.C.03	Requirement for ITSMs	Where an agency is spread across a number of geographical sites, it is recommended that the agency SHOULD appoint a local ITSM at each major site.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.3.4.C.04	Requirement for ITSMs	The ITSM role SHOULD be undertaken by personnel with an appropriate level of authority and training based on the size of the agency or their area of responsibility within the agency.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.3.4.C.05	Requirement for ITSMs	ITSMs SHOULD NOT have additional responsibilities beyond those needed to fulfil the role as outlined within this manual.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.3.5.C.01	Responsibilities - Security programs	ITSMs SHOULD work with the CISO to develop an information security program within the agency.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.3.5.C.02	Responsibilities - Security programs	ITSMs SHOULD undertake and manage projects to address identified security risks.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
3.3.6.C.01	Responsibilities - Working with ICT projects	ITSMs MUST be responsible for assisting system owners to obtain and maintain the accreditation of their systems.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.3.6.C.02	Responsibilities - Working with ICT projects	ITSMs SHOULD identify systems that require security measures and assist in the selection of appropriate information security measures for such systems.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.3.6.C.03	Responsibilities - Working with ICT projects	ITSMs SHOULD consult with ICT project personnel to ensure that information security is included in the evaluation, selection, installation, configuration and operation of IT equipment and software.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.3.6.C.04	Responsibilities - Working with ICT projects	ITSMs SHOULD work with agency enterprise architecture teams to ensure that security risk assessments are incorporated into system architectures and to identify, evaluate and select information security solutions to meet the agency's security objectives.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.3.6.C.05	Responsibilities - Working with ICT projects	ITSMs SHOULD be included in the agency's change management and change control processes to ensure that risks are properly identified and controls are properly applied to manage those risks.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.3.6.C.06	Responsibilities - Working with ICT projects	ITSMs SHOULD notify the Accreditation Authority of any significant change that may affect the accreditation of that system.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.3.7.C.01	Responsibilities - Working with vendors	ITSMs SHOULD liaise with vendors and agency purchasing and legal areas to establish mutually acceptable information security contracts and service-level agreements.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.3.8.C.01	Responsibilities - Implementing security	ITSMs MUST be responsible for ensuring the development, maintenance, updating and implementation of Security Risk Management Plans (SRMPs), Systems Security Plans (SSP) and any Standard Operating Procedures (SOPs) for all agency systems.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.3.8.C.02	Responsibilities - Implementing security	ITSMs SHOULD conduct security risk assessments on the implementation of new or updated IT equipment or software in the existing environment and develop treatment strategies if necessary.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.3.8.C.03	Responsibilities - Implementing security	ITSMs SHOULD select and coordinate the implementation of controls to support and enforce information security policies.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.3.8.C.04	Responsibilities - Implementing security	ITSMs SHOULD provide leadership and direction for the integration of information security strategies and architecture with agency business and ICT strategies and architecture.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.3.8.C.05	Responsibilities - Implementing security	ITSMs SHOULD provide technical and managerial expertise for the administration of information security management tools.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.3.9.C.01	Responsibilities - Budgeting	ITSMs SHOULD work with the CISO to develop information security budget projections and resource allocations based on short-term and long-term goals and objectives.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.3.10.C.01	Responsibilities - Reporting	ITSMs SHOULD coordinate, measure and report on technical aspects of information security management.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.3.10.C.02	Responsibilities - Reporting	ITSMs SHOULD monitor and report on compliance with information security policies, as well as the enforcement of information security policies within the agency.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.3.10.C.03	Responsibilities - Reporting	ITSMs SHOULD provide regular reports on information security incidents and other areas of particular concern to the CISO.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.3.10.C.04	Responsibilities - Reporting	ITSMs SHOULD assess and report on threats, vulnerabilities, and residual security risks and recommend remedial actions.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.3.11.C.01	Responsibilities - Auditing	ITSMs SHOULD assist system owners and security personnel in understanding and responding to audit failures reported by auditors.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.3.12.C.01	Responsibilities - Disaster recovery	ITSMs SHOULD assist and guide the disaster recovery planning team in the selection of recovery strategies and the development, testing and maintenance of disaster recovery plans.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.3.13.C.01	Responsibilities - Training	ITSMs SHOULD provide or arrange for the provision of information security awareness and training for all agency personnel.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.3.13.C.02	Responsibilities - Training	ITSMs SHOULD develop technical information materials and workshops on information security trends, threats, good practices and control mechanisms as appropriate.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.3.14.C.01	Responsibilities - Providing security knowledge	ITSMs SHOULD maintain a current and up-to-date security knowledge base comprising of a technical reference library, security advisories and alerts, information on information security trends and practices, and relevant laws, regulations, standards and guidelines.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.3.14.C.02	Responsibilities - Providing security knowledge	ITSMs SHOULD provide expert guidance on security matters for ICT projects.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.3.14.C.03	Responsibilities - Providing security knowledge	ITSMs SHOULD provide technical advice for the information security steering committee, change management committee and other agency and inter-agency committees as required.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.3.15.C.01	Responsibilities	The ITSM SHOULD keep the CISO and system owners informed with up-to-date information on current threats.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.4.10.C.01	Requirement for system owners	Each system MUST have a system owner who is responsible for the operation and maintenance of the system.	Functional	Intersects With	System Administrative Processes	AST-26	Mechanisms exist to develop, implement and govern system administration processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining Technology Assets, Applications and/or Services (TAAS).	5	
3.4.10.C.01	Requirement for system owners	Each system MUST have a system owner who is responsible for the operation and maintenance of the system.	Functional	Intersects With	Database Administrative Processes	AST-28	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	5	
3.4.10.C.01	Requirement for system owners	Each system MUST have a system owner who is responsible for the operation and maintenance of the system.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.4.10.C.01	Requirement for system owners	Each system MUST have a system owner who is responsible for the operation and maintenance of the system.	Functional	Intersects With	Documentation Requirements	TDA-04	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	
3.4.10.C.02	Requirement for system owners	System owners SHOULD be a member of the Senior Executive Team or an equivalent management position, for large or critical agency systems.	Functional	Intersects With	System Administrative Processes	AST-26	Mechanisms exist to develop, implement and govern system administration processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining Technology Assets, Applications and/or Services (TAAS).	5	
3.4.10.C.02	Requirement for system owners	System owners SHOULD be a member of the Senior Executive Team or an equivalent management position, for large or critical agency systems.	Functional	Intersects With	Database Administrative Processes	AST-28	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	5	
3.4.10.C.02	Requirement for system owners	System owners SHOULD be a member of the Senior Executive Team or an equivalent management position, for large or critical agency systems.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3.4.10.C.02	Requirement for system owners	System owners SHOULD be a member of the Senior Executive Team or an equivalent management position, for large or critical agency systems.	Functional	Intersects With	Documentation Requirements	TDA-04	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	
3.4.11.C.01	Accreditation responsibilities	System owners MUST obtain and maintain accreditation of their system(s).	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	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	
3.4.11.C.01	Accreditation responsibilities	System owners MUST obtain and maintain accreditation of their system(s).	Functional	Intersects With	Implement Controls	GOV-15.2	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	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
3.4.12.C.01	Documentation responsibilities	System owners MUST ensure the development, maintenance and implementation of complete, accurate and up to date Information Security documentation for systems under their ownership. Such actions MUST be documented.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	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	
3.4.12.C.01	Documentation responsibilities	System owners MUST ensure the development, maintenance and implementation of complete, accurate and up to date Information Security documentation for systems under their ownership. Such actions MUST be documented.	Functional	Subset Of	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	10	
3.4.12.C.02	Documentation responsibilities	System Owners MUST involve the ITSM in the redevelopment and updates of the Information Security documentation.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	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	
3.4.12.C.02	Documentation responsibilities	System Owners MUST involve the ITSM in the redevelopment and updates of the Information Security documentation.	Functional	Subset Of	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	10	
3.5.4.C.01	Responsibilities of system users	All system users MUST comply with the relevant security policies and procedures for the systems they use.	Functional	Intersects With	Terms of Employment	HRS-05	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	
3.5.4.C.01	Responsibilities of system users	All system users MUST comply with the relevant security policies and procedures for the systems they use.	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	
3.5.4.C.02	Responsibilities of system users	All system users MUST: protect account authenticators at the same classification of the system it secures; not share authenticators for accounts without approval; be responsible for all actions under their accounts; and use their access to only perform authorised tasks and functions.	Functional	Intersects With	Terms of Employment	HRS-05	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	
3.5.4.C.02	Responsibilities of system users	All system users MUST: protect account authenticators at the same classification of the system it secures; not share authenticators for accounts without approval; be responsible for all actions under their accounts; and use their access to only perform authorised tasks and functions.	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	
3.5.4.C.03	Responsibilities of system users	System users that need to bypass security policies, procedures or mechanisms for any reason MUST seek formal authorisation from the CISO or the ITSM if this authority has been specifically delegated to the ITSM.	Functional	Intersects With	Terms of Employment	HRS-05	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	
3.5.4.C.03	Responsibilities of system users	System users that need to bypass security policies, procedures or mechanisms for any reason MUST seek formal authorisation from the CISO or the ITSM if this authority has been specifically delegated to the ITSM.	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	
4.2.10.C.01	Certification Audit	All systems MUST undergo an audit as part of the certification process.	Functional	Intersects With	Assessments	IAO-02	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	
4.2.11.C.01	Certification decision	The certification authority MUST accept that the controls are appropriate, effective and comply with the Protective Security Requirements (PSR) and in particular the relevant NZISM components, in order to award certification.	Functional	Intersects With	Security Assessment Report (SAR)	IAO-02.4	Mechanisms exist to produce a Security Assessment Report (SAR) at the conclusion of a security assessment to certify the results of the assessment and assist with any remediation actions.	5	
4.2.11.C.01	Certification decision	The certification authority MUST accept that the controls are appropriate, effective and comply with the Protective Security Requirements (PSR) and in particular the relevant NZISM components, in order to award certification.	Functional	Intersects With	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	5	
4.2.12.C.01	Residual security risk assessment	Following the audit, the certification authority SHOULD produce an assessment for the Accreditation Authority outlining the residual security risks relating to the operation of the system and a recommendation on whether to award accreditation or not.	Functional	Intersects With	Security Assessment Report (SAR)	IAO-02.4	Mechanisms exist to produce a Security Assessment Report (SAR) at the conclusion of a security assessment to certify the results of the assessment and assist with any remediation actions.	5	
4.2.12.C.01	Residual security risk assessment	Following the audit, the certification authority SHOULD produce an assessment for the Accreditation Authority outlining the residual security risks relating to the operation of the system and a recommendation on whether to award accreditation or not.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-05	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	
4.3.16.C.01	Independence of auditors	Agencies SHOULD ensure that auditors conducting audits are able to demonstrate independence and are not also the system owner or certification authority.	Functional	Intersects With	Control Conformity Monitoring	CPL-03	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	
4.3.16.C.01	Independence of auditors	Agencies SHOULD ensure that auditors conducting audits are able to demonstrate independence and are not also the system owner or certification authority.	Functional	Intersects With	Assessor Independence	IAO-02.1	Mechanisms exist to ensure assessors or assessment teams have the appropriate independence to conduct security, compliance and/or resilience control assessments.	5	
4.3.16.C.01	Independence of auditors	Agencies SHOULD ensure that auditors conducting audits are able to demonstrate independence and are not also the system owner or certification authority.	Functional	Intersects With	Third-Party Assessment Reciprocity	IAO-02.3	Mechanisms exist to accept and respond to the results of external assessments that are performed by impartial, external organizations.	5	
4.3.17.C.01	Audit preparation	Prior to undertaking the audit the system owner MUST approve the system architecture and associated information security documentation.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	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	
4.3.18.C.01	Audit (first stage)	The SecPol, SRMP, SSP, SOPs and IRP documentation MUST be reviewed by the auditor to ensure that it is comprehensive and appropriate for the environment the system is to operate within.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	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	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
4.3.18.C.02	Audit (first stage)	The Information Security Policy (SecPol) MUST be reviewed by the auditor to ensure that all applicable controls specified in this manual are addressed.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	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	
4.3.18.C.03	Audit (first stage)	The system and security architecture (including information security documentation) SHOULD be reviewed by the auditor to ensure that it is based on sound information security principles and meets information security requirements, including the NZISM.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	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	
4.3.18.C.04	Audit (first stage)	The Information Security Policy (SecPol) SHOULD be reviewed by the auditor to ensure that policies have been developed or identified by the agency to protect classified information that is processed, stored or communicated by its systems.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	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	
4.3.18.C.05	Audit (first stage)	The system owner SHOULD provide a statement of applicability for the system which includes the following topics: the baseline of this manual used for determining controls; controls that are, and are not, applicable to the system; controls that are applicable but are not being complied with; and any additional controls implemented as a result of the SRMP.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	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	
4.3.19.C.01	Implementing controls	Prior to undertaking any system testing in support of the certification process, the system owner MUST implement the controls for the system.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
4.3.19.C.01	Implementing controls	Prior to undertaking any system testing in support of the certification process, the system owner MUST implement the controls for the system.	Functional	Intersects With	Assignment of Responsibility	CFG-01.1	Mechanisms exist to implement a segregation of duties for configuration management that prevents developers from performing production configuration management duties.	5	
4.3.19.C.01	Implementing controls	Prior to undertaking any system testing in support of the certification process, the system owner MUST implement the controls for the system.	Functional	Intersects With	Centralized Management of Security, Compliance & Resilience Controls	SEA-01.1	Mechanisms exist to centrally-manage the organization-wide management and implementation of security, compliance and resilience controls and related processes.	5	
4.3.20.C.01	Audit (second stage)	The implementation of controls MUST be assessed to determine whether they have been implemented correctly and are operating effectively.	Functional	Intersects With	Assessments	IAO-02	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	
4.3.20.C.01	Audit (second stage)	The implementation of controls MUST be assessed to determine whether they have been implemented correctly and are operating effectively.	Functional	Intersects With	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; (11) Artificial Intelligence and Autonomous Technologies (AAT); and/or	5	
4.3.20.C.01	Audit (second stage)	The implementation of controls MUST be assessed to determine whether they have been implemented correctly and are operating effectively.	Functional	Intersects With	Third-Party Assessment Reciprocity	IAO-02.3	Mechanisms exist to accept and respond to the results of external assessments that are performed by impartial, external organizations.	5	
4.3.20.C.02	Audit (second stage)	The auditor MUST ensure that, where applicable, a physical security certification has been awarded by an appropriate physical security certification authority.	Functional	Intersects With	Assessments	IAO-02	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	
4.3.20.C.02	Audit (second stage)	The auditor MUST ensure that, where applicable, a physical security certification has been awarded by an appropriate physical security certification authority.	Functional	Intersects With	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; (11) Artificial Intelligence and Autonomous Technologies (AAT); and/or	5	
4.3.20.C.02	Audit (second stage)	The auditor MUST ensure that, where applicable, a physical security certification has been awarded by an appropriate physical security certification authority.	Functional	Intersects With	Third-Party Assessment Reciprocity	IAO-02.3	Mechanisms exist to accept and respond to the results of external assessments that are performed by impartial, external organizations.	5	
4.3.20.C.03	Audit (second stage)	The physical security certification SHOULD be less than three (3) years old at the time of the audit.	Functional	Intersects With	Assessments	IAO-02	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	
4.3.20.C.03	Audit (second stage)	The physical security certification SHOULD be less than three (3) years old at the time of the audit.	Functional	Intersects With	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; (11) Artificial Intelligence and Autonomous Technologies (AAT); and/or	5	
4.3.20.C.03	Audit (second stage)	The physical security certification SHOULD be less than three (3) years old at the time of the audit.	Functional	Intersects With	Third-Party Assessment Reciprocity	IAO-02.3	Mechanisms exist to accept and respond to the results of external assessments that are performed by impartial, external organizations.	5	
4.3.21.C.01	Report of compliance	The auditor MUST produce a report of compliance for the certification authority outlining areas of non-compliance for a system and any suggested remediation actions.	Functional	Intersects With	Security Assessment Report (SAR)	IAO-02.4	Mechanisms exist to produce a Security Assessment Report (SAR) at the conclusion of a security assessment to certify the results of the assessment and assist with any remediation actions.	5	
4.4.4.C.01	Accreditation framework	Agencies MUST develop an accreditation framework for their agency.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
4.4.5.C.01	Accreditation	Agencies MUST ensure that each of their systems is awarded accreditation.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
4.4.5.C.02	Accreditation	Agencies MUST ensure that all systems are awarded accreditation before they are used operationally.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
4.4.5.C.03	Accreditation	Agencies MUST ensure that all systems are awarded accreditation prior to connecting them to any other internal or external system.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
4.4.5.C.04	Accreditation	Agencies SHOULD ensure information security monitoring, logging and auditing is conducted on all accredited systems.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
4.4.6.C.01	Determining authorities	For multi-national and multi-agency systems, the Certification and Accreditation Authorities SHOULD be determined by a formal agreement between the parties involved.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
4.4.7.C.01	Notifying authorities	Prior to beginning the accreditation process the system owner SHOULD advise the certification and accreditation authorities of their intent to seek certification and accreditation for their system.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
4.4.7.C.02	Notifying authorities	Agencies SHOULD confirm governance arrangements with the certification authorities, and with the accreditation authorities.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
4.4.8.C.01	Due diligence	Where an agency's system exchanges information with a third-party system, the agency MUST ensure that the receiving party has appropriate measures in place to provide a level of protection commensurate with the classification or privacy requirements of their information and that the third party is authorised to receive that information.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
4.4.8.C.02	Due diligence	An agency MUST ensure that a third party is aware of the agency's information security expectations and national security requirements by defining expectations in documentation that includes, but is not limited to: contract provisions; a memorandum of understanding; non-disclosure agreements.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
4.4.8.C.03	Due diligence	An agency MUST ensure that a third party complies with the agency's information security expectations through a formal process providing assurance to agency management that the operation of information security within the third party meets, and continues to meet, these expectations.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
4.4.8.C.04	Due diligence	Agencies SHOULD review accreditation deliverables when determining whether the receiving party has appropriate measures in place to provide a level of protection commensurate with the classification of their information.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
4.4.9.C.01	Processing restrictions	Agencies MUST NOT allow a system to process, store or communicate classified information above the classification for which the system has received accreditation.	Functional	Intersects With	Highest Classification Level	DCH-02.1	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	
4.4.9.C.01	Processing restrictions	Agencies MUST NOT allow a system to process, store or communicate classified information above the classification for which the system has received accreditation.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
4.4.10.C.01	Accrediting systems bearing a compartment marking	A system that processes, stores or communicates compartmented information MUST be accredited by the GCSB.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
4.4.10.C.01	Accrediting systems bearing a compartment marking	A system that processes, stores or communicates compartmented information MUST be accredited by the GCSB.	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
4.4.10.C.01	Accrediting systems bearing a compartment marking	A system that processes, stores or communicates compartmented information MUST be accredited by the GCSB.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
4.4.11.C.01	Requirement for New Zealand control	Agencies MUST ensure that systems processing, storing or communicating NZEO information remain under the control of a New Zealand national working for the New Zealand government, at all times.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
4.4.12.C.01	Reaccreditation	Agencies MUST ensure that the period between accreditations of each of their systems does not exceed three years.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
4.4.12.C.02	Reaccreditation	Agencies MUST notify associated agencies where multiple agencies are connected to agency systems operating with expired accreditations.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
4.4.12.C.03	Reaccreditation	Agencies MUST notify the Government Chief Digital Officer (GCDO) where All-of-Government systems are connected to agency systems operating with expired accreditations.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
4.4.12.C.04	Reaccreditation	Agencies MUST NOT operate a system without accreditation or with a lapsed accreditation unless the accreditation authority has granted a dispensation.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
4.4.12.C.05	Reaccreditation	Agencies SHOULD ensure that the period between accreditations of each of their systems does not exceed two years.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
4.5.17.C.01	Certification	All systems MUST be certified as part of the accreditation process.	Functional	Intersects With	Security Assessment Report (SAR)	IAO-02.4	Mechanisms exist to produce a Security Assessment Report (SAR) at the conclusion of a security assessment to certify the results of the assessment and assist with any remediation actions.	5	
4.5.18.C.01	Accreditation decision	The Accreditation Authority MUST accept the residual security risk relating to the operation of a system in order to award accreditation.	Functional	Intersects With	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	5	
4.5.18.C.02	Accreditation decision	The Accreditation Authority MUST advise other agencies where the accreditation decision may affect those agencies.	Functional	Intersects With	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	5	
4.5.18.C.03	Accreditation decision	The Accreditation Authority MUST advise the GCDO where the accreditation decision may affect any All-of-Government systems.	Functional	Intersects With	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	5	
5.1.7.C.01	Information Security Policy (SecPol)	Agencies MUST have a SecPol for their agency. The SecPol is usually sponsored by the Chief Executive and managed by the CISO or Chief Information Officer (CIO). The ITSM should be the custodian of the SecPol. The SecPol should include an acceptable use policy for any agency technology equipment, systems, resources and data.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
5.1.8.C.01	Systems Architecture	All systems MUST have a documented Systems Architecture.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	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	
5.1.9.C.01	Security Risk Management Plan (SRMP)	Agencies MUST ensure that every system is covered by a Security Risk Management Plan, which includes identification of risk owners.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	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	
5.1.9.C.01	Security Risk Management Plan (SRMP)	Agencies MUST ensure that every system is covered by a Security Risk Management Plan, which includes identification of risk owners.	Functional	Subset Of	Risk Management Program	RSK-01	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	
5.1.10.C.01	System Security Plan (SSP)	Agencies MUST ensure that every system is covered by a SSP.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	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	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
5.1.11.C.01	Standard Operating Procedures (SOPs)	Agencies MUST ensure that Standard Operating Procedures (SOPs) are developed for systems.	Functional	Intersects With	System Administrative Processes	AST-26	Mechanisms exist to develop, implement and govern system administration processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining Technology Assets, Applications and/or Services (TAAS).	5	
5.1.11.C.01	Standard Operating Procedures (SOPs)	Agencies MUST ensure that Standard Operating Procedures (SOPs) are developed for systems.	Functional	Intersects With	Database Administrative Processes	AST-28	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	5	
5.1.11.C.01	Standard Operating Procedures (SOPs)	Agencies MUST ensure that Standard Operating Procedures (SOPs) are developed for systems.	Functional	Subset Of	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	10	
5.1.12.C.01	Incident Response Plan (IRP)	Agencies MUST develop an Incident Response Plan and supporting procedures.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
5.1.12.C.02	Incident Response Plan (IRP)	Agency personnel MUST be trained in and periodically exercise the Incident Response Plan.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
5.1.13.C.01	Emergency Procedures (EP)	Agencies SHOULD document procedures relating to securing classified information and systems when required to evacuate a facility in the event of an emergency.	Functional	Intersects With	System Administrative Processes	AST-26	Mechanisms exist to develop, implement and govern system administration processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining Technology Assets, Applications and/or Services (TAAS).	5	
5.1.13.C.01	Emergency Procedures (EP)	Agencies SHOULD document procedures relating to securing classified information and systems when required to evacuate a facility in the event of an emergency.	Functional	Intersects With	Database Administrative Processes	AST-28	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	5	
5.1.13.C.01	Emergency Procedures (EP)	Agencies SHOULD document procedures relating to securing classified information and systems when required to evacuate a facility in the event of an emergency.	Functional	Subset Of	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	10	
5.1.14.C.01	Developing content	Agencies SHOULD ensure that information security documentation is developed by personnel with a good understanding of policy requirements, the subject matter, essential processes and the agency's business and operations	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
5.1.14.C.01	Developing content	Agencies SHOULD ensure that information security documentation is developed by personnel with a good understanding of policy requirements, the subject matter, essential processes and the agency's business and operations	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
5.1.14.C.01	Developing content	Agencies SHOULD ensure that information security documentation is developed by personnel with a good understanding of policy requirements, the subject matter, essential processes and the agency's business and operations	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	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	
5.1.14.C.01	Developing content	Agencies SHOULD ensure that information security documentation is developed by personnel with a good understanding of policy requirements, the subject matter, essential processes and the agency's business and operations	Functional	Intersects With	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	5	
5.1.15.C.01	Documentation content	Agencies SHOULD ensure that their SRMP, Systems Architecture, SSP, SOPs and IRP are logically connected and consistent for each system, other agency systems and with the agency's SecPol.	Functional	Intersects With	Security Concept Of Operations (CONOPS)	OPS-02	Mechanisms exist to develop a security Concept of Operations (CONOPS), or a similarly-defined plan for achieving cybersecurity objectives, that documents management, operational and technical measures implemented to apply defense-in-depth techniques that is communicated to all appropriate stakeholders.	5	
5.1.16.C.01	Documentation framework	Agencies SHOULD create and maintain an overarching document describing the agency's documentation framework, including a complete listing of all information security documentation that shows a document hierarchy and defines how each document is related to the other.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
5.1.16.C.01	Documentation framework	Agencies SHOULD create and maintain an overarching document describing the agency's documentation framework, including a complete listing of all information security documentation that shows a document hierarchy and defines how each document is related to the other.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8	
5.1.16.C.02	Documentation framework	Where an agency lacks an existing, well-defined documentation framework, they SHOULD use the document names defined in this manual.	Functional	Intersects With	Secure Practices Alignment Justification	GOV-01.4	Mechanisms exist to align the organization's Security, Compliance & Resilience Program (SCRP) with one or more industry-recognized frameworks that: (1) Support external scrutiny; and	8	
5.1.16.C.02	Documentation framework	Where an agency lacks an existing, well-defined documentation framework, they SHOULD use the document names defined in this manual.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8	
5.1.17.C.01	Documentation Consistency	Where an agency uses alternative documentation names to those defined within this manual for their information security documentation they SHOULD convert the documentation names to those used in this manual.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
5.1.18.C.01	Documentation Classification	Agencies MUST ensure that their SecPol, SRMP, SSP, SOPs and IRP are appropriately classified.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
5.1.19.C.01	Outsourcing development of content	When information security documentation development is outsourced, agencies SHOULD: review the documents for suitability; retain control over the content; and ensure that all policy requirements are met.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8	
5.1.20.C.01	Obtaining formal sign-off	All information security documentation SHOULD be formally approved and signed off by a person with an appropriate level of seniority and authority.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
5.1.20.C.02	Obtaining formal sign-off	Agencies SHOULD ensure that: all high-level information security documentation is approved by the CISO and the agency head or their delegate; and all system-specific documents are reviewed by the ITSM and approved by the system owner.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
5.1.21.C.01	Documentation Maintenance	Agencies SHOULD develop a regular schedule for reviewing all information security documentation.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	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	
5.1.21.C.02	Documentation Maintenance	Agencies SHOULD ensure that information security documentation is reviewed: at least annually; or in response to significant changes in the environment, business or system; and with the date of the most recent review being recorded on each document.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	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	
5.2.3.C.01	The Information Security Policy (SecPol)	The Information Security Policy (SecPol) SHOULD document the information security guidelines, standards and responsibilities of an agency.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
5.2.3.C.02	The Information Security Policy (SecPol)	The Information Security Policy (SecPol) SHOULD include topics such as: accreditation processes; personnel responsibilities; configuration control; access control; networking and connections with other systems; physical security and media control; emergency procedures and information security incident management; vulnerability disclosure; change management; and information security awareness and training.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
5.3.6.C.01	Agency and system specific security risks	Agencies SHOULD determine agency and system specific security risks that could warrant additional controls to those specified in this manual.	Functional	Subset Of	Risk Management Program	RSK-01	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	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
5.3.7.C.01	Contents of SRMPs	The Security Risk Management Plan SHOULD contain a security risk assessment and a corresponding treatment strategy.	Functional	Subset Of	Risk Management Program	RSK-01	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	
5.3.8.C.01	Agency risk management	Agencies SHOULD incorporate their SRMP into their wider agency risk management plan.	Functional	Subset Of	Risk Management Program	RSK-01	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	
5.3.9.C.01	Risk Management standards	Agencies SHOULD develop their SRMP in accordance with international standards for risk management.	Functional	Subset Of	Risk Management Program	RSK-01	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	
5.4.5.C.01	Contents of System Security Plans (SSPs)	Agencies MUST select controls from this manual to be included in the SSP based on the scope of the system with additional system specific controls being included as a result of the associated SRMP. Encryption Key Management requires specific consideration; refer to Chapter 17 - Cryptography.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	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	
5.4.5.C.02	Contents of System Security Plans (SSPs)	Agencies SHOULD use the latest baseline of this manual when developing, and updating, their SSPs as part of the certification, accreditation and reaccreditation of their systems.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	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	
5.4.5.C.03	Contents of System Security Plans (SSPs)	Agencies SHOULD include a Key Management Plan in the SSP.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	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	
5.5.3.C.01	Development of SOPs	Agencies SHOULD develop SOPs for each of the following roles: ITSM; system administrator; and system user.	Functional	Intersects With	System Administrative Processes	AST-26	Mechanisms exist to develop, implement and govern system administration processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining Technology Assets, Applications and/or Services (TAAS).	5	
5.5.3.C.01	Development of SOPs	Agencies SHOULD develop SOPs for each of the following roles: ITSM; system administrator; and system user.	Functional	Intersects With	Database Administrative Processes	AST-28	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	5	
5.5.3.C.01	Development of SOPs	Agencies SHOULD develop SOPs for each of the following roles: ITSM; system administrator; and system user.	Functional	Subset Of	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	10	
5.5.4.C.01	ITSM SOPs	The following procedures SHOULD be documented in the ITSMs SOPs. Topic Procedures to be included Access control Authorising access rights to applications and data. Asset Musters Labelling, registering and mustering assets, including media. Audit logs Reviewing system audit trails and manual logs, particularly for privileged users. Configuration control Approving and releasing changes to the system software or configurations. Information security incidents Detecting, reporting and managing potential information security incidents. Establishing the cause of any information security incident, whether accidental or deliberate. Actions to be taken to recover and minimise the exposure from an information security incident. Additional actions to prevent reoccurrence. Data transfers Managing the review of media containing classified information that is to be transferred off-site. Managing the review of incoming media for malware or unapproved software. IT equipment	Functional	Intersects With	System Administrative Processes	AST-26	Mechanisms exist to develop, implement and govern system administration processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining Technology Assets, Applications and/or Services (TAAS).	5	
5.5.4.C.01	ITSM SOPs	The following procedures SHOULD be documented in the ITSMs SOPs. Topic Procedures to be included Access control Authorising access rights to applications and data. Asset Musters Labelling, registering and mustering assets, including media. Audit logs Reviewing system audit trails and manual logs, particularly for privileged users. Configuration control Approving and releasing changes to the system software or configurations. Information security incidents Detecting, reporting and managing potential information security incidents. Establishing the cause of any information security incident, whether accidental or deliberate. Actions to be taken to recover and minimise the exposure from an information security incident. Additional actions to prevent reoccurrence. Data transfers Managing the review of media containing classified information that is to be transferred off-site. Managing the review of incoming media for malware or unapproved software. IT equipment	Functional	Intersects With	Database Administrative Processes	AST-28	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	5	

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
5.5.4.C.01	ITSM SOPs	The following procedures SHOULD be documented in the ITSMs SOPs. Topic Procedures to be included Access control Authorising access rights to applications and data. Asset Musters Labelling, registering and mustering assets, including media. Audit logs Reviewing system audit trails and manual logs, particularly for privileged users. Configuration control Approving and releasing changes to the system software or configurations. Information security incidents Detecting, reporting and managing potential information security incidents. Establishing the cause of any information security incident, whether accidental or deliberate. Actions to be taken to recover and minimise the exposure from an information security incident. Additional actions to prevent reoccurrence. Data transfers Managing the review of media containing classified information that is to be transferred off-site. Managing the review of incoming media for malware or unapproved software. IT equipment	Functional	Subset Of	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	10	
5.5.5.C.01	System Administrator SOPs	The following procedures SHOULD be documented in the system administrators SOPs. Topic Procedures to be included Access control Implementing access rights to applications and data. Configuration control Implementing changes to the system software or configurations. System backup and recovery Backing up data, including audit logs. Securing backup tapes. Recovering from system failures. User account management Adding and removing system users. Setting system user privileges. Cleaning up directories and files when a system user departs or changes roles. Incident response Detecting, reporting and managing potential information security incidents. Establishing the cause of any information security incident, whether accidental or deliberate. Actions to be taken to recover and minimise the exposure from information	Functional	Intersects With	System Administrative Processes	AST-26	Mechanisms exist to develop, implement and govern system administration processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining Technology Assets, Applications and/or Services (TAAS).	5	
5.5.5.C.01	System Administrator SOPs	The following procedures SHOULD be documented in the system administrators SOPs. Topic Procedures to be included Access control Implementing access rights to applications and data. Configuration control Implementing changes to the system software or configurations. System backup and recovery Backing up data, including audit logs. Securing backup tapes. Recovering from system failures. User account management Adding and removing system users. Setting system user privileges. Cleaning up directories and files when a system user departs or changes roles. Incident response Detecting, reporting and managing potential information security incidents. Establishing the cause of any information security incident, whether accidental or deliberate. Actions to be taken to recover and minimise the exposure from information	Functional	Intersects With	Database Administrative Processes	AST-28	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	5	
5.5.5.C.01	System Administrator SOPs	The following procedures SHOULD be documented in the system administrators SOPs. Topic Procedures to be included Access control Implementing access rights to applications and data. Configuration control Implementing changes to the system software or configurations. System backup and recovery Backing up data, including audit logs. Securing backup tapes. Recovering from system failures. User account management Adding and removing system users. Setting system user privileges. Cleaning up directories and files when a system user departs or changes roles. Incident response Detecting, reporting and managing potential information security incidents. Establishing the cause of any information security incident, whether accidental or deliberate. Actions to be taken to recover and minimise the exposure from information	Functional	Subset Of	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	10	

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
5.5.6.C.01	System User SOPs	The following procedures SHOULD be documented in the system users SOPs. Topic Procedures to be included Acceptable Use Acceptable uses of the system(s). End of day How to secure systems at the end of the day. Information security incidents What to do in the case of a suspected or actual information security incident. Media control Procedures for handling and using media. Passwords Choosing and protecting passwords. Temporary absence How to secure systems when temporarily absent.	Functional	Intersects With	System Administrative Processes	AST-26	Mechanisms exist to develop, implement and govern system administration processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining Technology Assets, Applications and/or Services (TAAS).	5	
5.5.6.C.01	System User SOPs	The following procedures SHOULD be documented in the system users SOPs. Topic Procedures to be included Acceptable Use Acceptable uses of the system(s). End of day How to secure systems at the end of the day. Information security incidents What to do in the case of a suspected or actual information security incident. Media control Procedures for handling and using media. Passwords Choosing and protecting passwords. Temporary absence How to secure systems when temporarily absent.	Functional	Intersects With	Database Administrative Processes	AST-28	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	5	
5.5.6.C.01	System User SOPs	The following procedures SHOULD be documented in the system users SOPs. Topic Procedures to be included Acceptable Use Acceptable uses of the system(s). End of day How to secure systems at the end of the day. Information security incidents What to do in the case of a suspected or actual information security incident. Media control Procedures for handling and using media. Passwords Choosing and protecting passwords. Temporary absence How to secure systems when temporarily absent.	Functional	Subset Of	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	10	
5.5.7.C.01	Agreement to abide by SOPs	ITSMs, system administrators and system users SHOULD sign a statement that they have read and agree to abide by their respective SOPs.	Functional	Intersects With	Terms of Employment	HRS-05	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	
5.5.7.C.01	Agreement to abide by SOPs	ITSMs, system administrators and system users SHOULD sign a statement that they have read and agree to abide by their respective SOPs.	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	
5.6.3.C.01	Contents of IRPs	Agencies MUST include, as a minimum, the following content within their IRP: broad guidelines on what constitutes an information security incident; the minimum level of information security incident response and investigation training for system users and system administrators; the authority responsible for initiating investigations of an information security incident; the steps necessary to ensure the integrity of evidence supporting an information security incident; the steps necessary to ensure that critical systems remain operational; when and how to formally report information security incidents; and national policy requirements for incident reporting (see Chapter 7 - Information Security Incidents).	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
5.6.3.C.02	Contents of IRPs	Agencies SHOULD include the following content within their IRP: clear definitions of the types of information security incidents that are likely to be encountered; the expected response to each information security incident type; the authority within the agency that is responsible for responding to information security incidents; the criteria by which the responsible authority would initiate or request formal, police investigations of an information security incident; which other agencies or authorities need to be informed in the event of an investigation being undertaken; and the details of the system contingency measures or a reference to these details if they are located in a separate document.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
5.7.4.C.01	Evacuating facilities	Agencies MUST include in procedures for personnel evacuating a facility the requirement to secure classified information and systems prior to the evacuation.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
5.7.4.C.01	Evacuating facilities	Agencies MUST include in procedures for personnel evacuating a facility the requirement to secure classified information and systems prior to the evacuation.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
5.8.61.C.01	Risk Assessment	Agencies MUST conduct a risk assessment in order to determine the type and level of independent assurance required to satisfy certification and accreditation requirements.	Functional	Intersects With	Assessment Boundaries	IAO-01.1	Mechanisms exist to establish the scope of assessments by defining the assessment boundary, according to people, processes and technology that directly or indirectly impact the confidentiality, integrity, availability and safety of the Technology Assets, Applications, Services and/or Data (TAASD) under review.	5	
5.8.61.C.02	Risk Assessment	In all cases where assurance on service provider operations cannot be obtained directly, agencies SHOULD obtain independent assurance reports.	Functional	Intersects With	Assessment Boundaries	IAO-01.1	Mechanisms exist to establish the scope of assessments by defining the assessment boundary, according to people, processes and technology that directly or indirectly impact the confidentiality, integrity, availability and safety of the Technology Assets, Applications, Services and/or Data (TAASD) under review.	5	
5.8.61.C.03	Risk Assessment	In order to address identified risk areas, agencies SHOULD obtain relevant assurance reports and service provider certifications to inform a risk assessment and Certification activities as well as other aspects of the certification processes such as evidence of controls effectiveness and remediation plans.	Functional	Intersects With	Assessment Boundaries	IAO-01.1	Mechanisms exist to establish the scope of assessments by defining the assessment boundary, according to people, processes and technology that directly or indirectly impact the confidentiality, integrity, availability and safety of the Technology Assets, Applications, Services and/or Data (TAASD) under review.	5	
5.8.62.C.01	Independent Assurance	Agencies MUST incorporate the results of any independent assurance reports into the agency Certification process, to understand the residual risk position and controls required to manage risk appropriately.	Functional	Intersects With	Third-Party Assessment Reciprocity	IAO-02.3	Mechanisms exist to accept and respond to the results of external assessments that are performed by impartial, external organizations.	5	
5.9.23.C.01	Vulnerability disclosure policy (VDP) Risk Assessment	An agency MUST undertake a risk assessment to determine which systems and services to include in the agency's VDP.	Functional	Intersects With	Risk Assessment	RSK-04	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	
5.9.23.C.01	Vulnerability disclosure policy (VDP) Risk Assessment	An agency MUST undertake a risk assessment to determine which systems and services to include in the agency's VDP.	Functional	Intersects With	Vulnerability Disclosure Program (VDP)	THR-06	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of Technology Assets, Applications and/or Services (TAAS) that receives unsolicited input from the public about vulnerabilities in organizational TAAS.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
5.9.24.C.01	Vulnerability disclosure policy (VDP) Essential Content	An agency MUST develop and publish a VDP.	Functional	Intersects With	Vulnerability Disclosure Program (VDP)	THR-06	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of Technology Assets, Applications and/or Services (TAAS) that receives unsolicited input from the public about vulnerabilities in organizational TAAS.	5	
5.9.24.C.02	Vulnerability disclosure policy (VDP) Essential Content	An agency's VDP MUST contain at least the following core content: A scoping statement listing the systems the policy applies to; Contact details; Secure communication options (including any public keys); Information the finder should include in the report; Acknowledgement of reports and a response time; Guidance on what forms of vulnerability testing are out of scope for reporters/finders (permitted activities); Reporters/finders agreeing to not share information about the vulnerability until the end of the disclosure period, in order to allow the agency to address any issues before they become public; Illegal activities are not permitted (specifying the relevant legislation, such as the Crimes Act); and Either that "Bug bounties" will not be paid for any discoveries, or it should provide information about the agency's bug bounty programme.	Functional	Intersects With	Vulnerability Disclosure Program (VDP)	THR-06	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of Technology Assets, Applications and/or Services (TAAS) that receives unsolicited input from the public about vulnerabilities in organizational TAAS.	5	
5.9.25.C.01	Vulnerability disclosure policy (VDP) Additional Content	An agency SHOULD publish a security.txt to permit secure communications and direct any reports to a specific agency resource, in accordance with the agency's VDP.	Functional	Intersects With	Vulnerability Disclosure Program (VDP)	THR-06	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of Technology Assets, Applications and/or Services (TAAS) that receives unsolicited input from the public about vulnerabilities in organizational TAAS.	5	
5.9.26.C.01	Vulnerability disclosure policy (VDP) Setting Expectations	An agency MUST commit to addressing disclosed vulnerabilities within the timeframe it sets in its policy.	Functional	Intersects With	Vulnerability Disclosure Program (VDP)	THR-06	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of Technology Assets, Applications and/or Services (TAAS) that receives unsolicited input from the public about vulnerabilities in organizational TAAS.	5	
5.9.26.C.02	Vulnerability disclosure policy (VDP) Setting Expectations	An agency's vulnerability disclosure timeframe SHOULD be set to no more than 90 days.	Functional	Intersects With	Vulnerability Disclosure Program (VDP)	THR-06	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of Technology Assets, Applications and/or Services (TAAS) that receives unsolicited input from the public about vulnerabilities in organizational TAAS.	5	
5.9.27.C.01	Vulnerability disclosure policy (VDP) Integration	Agencies MUST ensure they integrate their VDP with other elements of their information security policies.	Functional	Intersects With	Vulnerability Disclosure Program (VDP)	THR-06	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of Technology Assets, Applications and/or Services (TAAS) that receives unsolicited input from the public about vulnerabilities in organizational TAAS.	5	
6.1.7.C.01	Conducting information security reviews	Agencies SHOULD undertake and document information security reviews of their systems at least annually.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
6.1.7.C.01	Conducting information security reviews	Agencies SHOULD undertake and document information security reviews of their systems at least annually.	Functional	Intersects With	Control Conformity Monitoring	CPL-03	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	
6.1.7.C.01	Conducting information security reviews	Agencies SHOULD undertake and document information security reviews of their systems at least annually.	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	5	
6.1.8.C.01	Managing Conflicts of Interest	Agencies SHOULD have information security reviews conducted by personnel independent to the target of the review or by an independent third party.	Functional	Intersects With	Independent Assessors	CPL-03.1	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	
6.1.9.C.01	Focus of information security reviews	Agencies SHOULD review the components detailed in the table below. Agencies SHOULD also ensure that any adjustments and changes as a result of any vulnerability analysis are consistent with the vulnerability disclosure policy. Component Review Information security documentation The SecPol, Systems Architecture, SRMPs, SSPs, SitePlan, SOPs, the VDP, the IRP, and any third party assurance reports. Dispensations Prior to the identified expiry date. Operating environment When an identified threat emerges or changes, an agency gains or loses a function or the operation of functions are moved to a new physical environment. Procedures After an information security incident or test exercise. System security Items that could affect the security of the system on a regular basis. Threats Changes in threat environment and risk profile. NZISM Changes to baseline or other controls, any new controls and guidance.	Functional	Intersects With	Control Conformity Monitoring	CPL-03	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	
6.1.9.C.01	Focus of information security reviews	Agencies SHOULD review the components detailed in the table below. Agencies SHOULD also ensure that any adjustments and changes as a result of any vulnerability analysis are consistent with the vulnerability disclosure policy. Component Review Information security documentation The SecPol, Systems Architecture, SRMPs, SSPs, SitePlan, SOPs, the VDP, the IRP, and any third party assurance reports. Dispensations Prior to the identified expiry date. Operating environment When an identified threat emerges or changes, an agency gains or loses a function or the operation of functions are moved to a new physical environment. Procedures After an information security incident or test exercise. System security Items that could affect the security of the system on a regular basis. Threats Changes in threat environment and risk profile. NZISM Changes to baseline or other controls, any new controls and guidance.	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	5	
6.2.4.C.01	Vulnerability analysis strategy	Agencies SHOULD implement a vulnerability analysis strategy by: monitoring public domain information about new vulnerabilities in operating systems and application software; considering the use of automated tools to perform vulnerability assessments on systems in a controlled manner; running manual checks against system configurations to ensure that only allowed services are active and that disallowed services are prevented; using security checklists for operating systems and common applications; and examining any significant incidents on the agency's systems.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
6.2.4.C.01	Vulnerability analysis strategy	Agencies SHOULD implement a vulnerability analysis strategy by: monitoring public domain information about new vulnerabilities in operating systems and application software; considering the use of automated tools to perform vulnerability assessments on systems in a controlled manner; running manual checks against system configurations to ensure that only allowed services are active and that disallowed services are prevented; using security checklists for operating systems and common applications; and examining any significant incidents on the agency's systems.	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	
6.2.5.C.01	Conducting vulnerability assessments	Agencies SHOULD conduct vulnerability assessments in order to establish a baseline. This SHOULD be done: before a system is first used; after any significant incident; after a significant change to the system; after changes to standards, policies and guidelines; when specified by an ITSM or system owner.	Functional	Intersects With	Threat Analysis & Flaw Remediation During Development	IAO-04	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	
6.2.5.C.01	Conducting vulnerability assessments	Agencies SHOULD conduct vulnerability assessments in order to establish a baseline. This SHOULD be done: before a system is first used; after any significant incident; after a significant change to the system; after changes to standards, policies and guidelines; when specified by an ITSM or system owner.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
6.2.6.C.01	Resolving vulnerabilities	Agencies SHOULD analyse and treat all vulnerabilities and subsequent security risks to their systems identified during a vulnerability assessment.	Functional	Intersects With	Threat Analysis & Flaw Remediation During Development	IAO-04	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	
6.2.6.C.01	Resolving vulnerabilities	Agencies SHOULD analyse and treat all vulnerabilities and subsequent security risks to their systems identified during a vulnerability assessment.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
6.2.6.C.01	Resolving vulnerabilities	Agencies SHOULD analyse and treat all vulnerabilities and subsequent security risks to their systems identified during a vulnerability assessment.	Functional	Intersects With	Continuous Vulnerability Remediation Activities	VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	5	
6.3.6.C.01	Change management	Agencies MUST ensure that for routine and urgent changes: the change management process, as defined in the relevant information security documentation, is followed; the proposed change is approved by the relevant authority; any proposed change that could impact the security or accreditation status of a system is submitted to the Accreditation Authority for approval; and all associated information security documentation is updated to reflect the change.	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
6.3.6.C.02	Change management	Agencies SHOULD ensure that for routine and urgent changes: the change management process, as defined in the relevant information security documentation, is followed; the proposed change is approved by the relevant authority; any proposed change that could impact the security of a system or accreditation status is submitted to the Accreditation Authority for approval; and all associated information security documentation is updated to reflect the change.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
6.3.7.C.01	Change management process	An agency's change management process MUST define appropriate actions to be followed before and after urgent changes are implemented.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
6.3.7.C.02	Change management process	An agency's change management process SHOULD define appropriate actions to be followed before and after urgent changes are implemented.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
6.3.7.C.03	Change management process	Agencies SHOULD follow this change management process outline: produce a written change request; submit the change request to all stakeholders for approval; document the changes to be implemented; test the approved changes; notification to user of the change schedule and likely effect or outage; implement the approved changes after successful testing; update the relevant information security documentation including the SRMP, SSP and SOPs notify and educate system users of the changes that have been implemented as close as possible to the time the change is applied; and continually educate system users in regards to changes.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
6.3.8.C.01	Changes impacting the security of a system	When a configuration change impacts the security of a system and is subsequently assessed as having changed the overall security risk for the system, the agency MUST reaccredit the system.	Functional	Intersects With	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	5	
6.3.8.C.01	Changes impacting the security of a system	When a configuration change impacts the security of a system and is subsequently assessed as having changed the overall security risk for the system, the agency MUST reaccredit the system.	Functional	Intersects With	Assessments	IAO-02	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	
6.3.8.C.01	Changes impacting the security of a system	When a configuration change impacts the security of a system and is subsequently assessed as having changed the overall security risk for the system, the agency MUST reaccredit the system.	Functional	Intersects With	Security Assessment Report (SAR)	IAO-02.4	Mechanisms exist to produce a Security Assessment Report (SAR) at the conclusion of a security assessment to certify the results of the assessment and assist with any remediation actions.	5	
6.3.8.C.01	Changes impacting the security of a system	When a configuration change impacts the security of a system and is subsequently assessed as having changed the overall security risk for the system, the agency MUST reaccredit the system.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-05	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	
6.4.5.C.01	Availability requirements	Agencies MUST determine availability and recovery requirements for their systems and implement measures consistent with the agency's SRMP to support them.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
6.4.6.C.01	Backup strategy	Agencies SHOULD: Identify vital records; backup all vital records; store copies of critical information, with associated documented recovery procedures, offsite and secured in accordance with the requirements for the highest classification of the information; and test backup and restoration processes regularly to confirm their effectiveness.	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
6.4.7.C.01	Business Continuity plan	Agencies SHOULD develop and document a business continuity plan.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
6.4.8.C.01	Disaster recovery plan	Agencies SHOULD develop and document a disaster recovery plan.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
7.1.7.C.01	Preventing and detecting information security incidents	Agencies MUST develop, implement and maintain tools and procedures covering the detection of potential information security incidents, incorporating: user awareness and training; counter-measures against malicious code, known attack methods and types; intrusion detection strategies; data egress monitoring & control; access control anomalies; audit analysis; system integrity checking; and vulnerability assessments.	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	
7.1.7.C.02	Preventing and detecting information security incidents	Agencies SHOULD develop, implement and maintain tools and procedures covering the detection of potential information security incidents, incorporating: user awareness and training; counter-measures against malicious code, known attack methods and types; intrusion detection strategies; dynamic network defence (i.e. protective DNS and/or NGFW) data egress monitoring & control; access control anomalies; audit analysis; system integrity checking; and vulnerability assessments.	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	
7.1.7.C.03	Preventing and detecting information security incidents	Agencies SHOULD use the results of the security risk assessment to determine the appropriate balance of resources allocated to prevention versus resources allocated to detection of information security incidents.	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	
7.2.18.C.01	Reporting information security incidents	Agencies MUST direct personnel to report information security incidents to an ITSM as soon as possible after the information security incident is discovered in accordance with agency procedures.	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	
7.2.18.C.01	Reporting information security incidents	Agencies MUST direct personnel to report information security incidents to an ITSM as soon as possible after the information security incident is discovered in accordance with agency procedures.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
7.2.18.C.01	Reporting information security incidents	Agencies MUST direct personnel to report information security incidents to an ITSM as soon as possible after the information security incident is discovered in accordance with agency procedures.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
7.2.18.C.01	Reporting information security incidents	Agencies MUST direct personnel to report information security incidents to an ITSM as soon as possible after the information security incident is discovered in accordance with agency procedures.	Functional	Intersects With	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations.	5	
7.2.18.C.01	Reporting information security incidents	Agencies MUST direct personnel to report information security incidents to an ITSM as soon as possible after the information security incident is discovered in accordance with agency procedures.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
7.2.18.C.01	Reporting information security incidents	Agencies MUST direct personnel to report information security incidents to an ITSM as soon as possible after the information security incident is discovered in accordance with agency procedures.	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive and/or regulated data incidents in a timely manner.	5	
7.2.18.C.02	Reporting information security incidents	Agencies SHOULD: encourage personnel to note and report any observed or suspected security weaknesses in, or threats to, systems or services; establish and follow procedures for reporting system, software or other malfunctions; put mechanisms in place to enable the types, volumes and costs of information security incidents and malfunctions to be quantified and monitored; and deal with the violation of agency information security policies and procedures by personnel through training and, where warranted, a formal disciplinary process.	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
7.2.18.C.02	Reporting information security incidents	Agencies SHOULD: encourage personnel to note and report any observed or suspected security weaknesses in, or threats to, systems or services; establish and follow procedures for reporting system, software or other malfunctions; put mechanisms in place to enable the types, volumes and costs of information security incidents and malfunctions to be quantified and monitored; and deal with the violation of agency information security policies and procedures by personnel through training and, where warranted, a formal disciplinary process.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
7.2.19.C.01	Responsibilities when reporting an information security incident	The ITSM MUST keep the CISO fully informed of information security incidents within an agency.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
7.2.20.C.01	Reporting information security incidents to National Cyber Security Centre (NCSC)	The Agency ITSM, MUST report information security incidents categorised as: Critical; Serious; or incidents related to multi-agency or government systems; to the NCSC as soon as possible. A Report Form is provided on the NCSC website under Reporting an Incident at Report an incident and request support | National Cyber Security Centre	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
7.2.20.C.01	Reporting information security incidents to National Cyber Security Centre (NCSC)	The Agency ITSM, MUST report information security incidents categorised as: Critical; Serious; or incidents related to multi-agency or government systems; to the NCSC as soon as possible. A Report Form is provided on the NCSC website under Reporting an Incident at Report an incident and request support | National Cyber Security Centre	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive and/or regulated data incidents in a timely manner.	5	
7.2.20.C.02	Reporting information security incidents to National Cyber Security Centre (NCSC)	Agencies SHOULD report information security incidents categorised as Low to the NCSC. A Report Form is provided on the NCSC website under Reporting an Incident at Report an incident and request support | National Cyber Security Centre	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	10	
7.2.20.C.03	Reporting information security incidents to National Cyber Security Centre (NCSC)	Agencies SHOULD formally share post-incident review reports by emailing them to incidents@ncsc.govt.nz.	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	10	
7.2.21.C.01	Outsourcing and information security incidents	Agencies that outsource their information technology services and functions MUST ensure that the service provider advises and consults with the agency when an information security incident occurs.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
7.2.21.C.01	Outsourcing and information security incidents	Agencies that outsource their information technology services and functions MUST ensure that the service provider advises and consults with the agency when an information security incident occurs.	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive and/or regulated data incidents in a timely manner.	5	
7.2.22.C.01	Cryptographic keying material	Agencies MUST notify all system users of any suspected or confirmed loss or compromise of keying material.	Functional	Intersects With	Supply Chain Coordination	IRO-10.4	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	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
7.2.22.C.01	Cryptographic keying material	Agencies MUST notify all system users of any suspected or confirmed loss or compromise of keying material.	Functional	Intersects With	Security Compromise Notification Agreements	TPM-05.1	Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely affected Technology Assets, Applications and/or Services (TAAS) that the organization utilizes.	5	
7.2.23.C.01	Replacement of Cryptographic Key (HACE) keying material	Agencies MUST replace compromised cryptographic keys as a matter of urgency and record the replacement in the incident reporting.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
7.2.23.C.01	Replacement of Cryptographic Key (HACE) keying material	Agencies MUST replace compromised cryptographic keys as a matter of urgency and record the replacement in the incident reporting.	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive and/or regulated data incidents in a timely manner.	5	
7.2.23.C.01	Replacement of Cryptographic Key (HACE) keying material	Agencies MUST replace compromised cryptographic keys as a matter of urgency and record the replacement in the incident reporting.	Functional	Intersects With	Security Compromise Notification Agreements	TPM-05.1	Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely affected Technology Assets, Applications and/or Services (TAAS) that the organization utilizes.	5	
7.2.24.C.01	High Assurance Cryptographic Equipment (HACE) keying material	Agencies MUST urgently notify GCSB of any suspected loss or compromise of keying material associated with HACE.	Functional	Intersects With	Cryptographic Key Loss or Change	CRY-09.3	Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users.	5	
7.3.5.C.01	Information security incident management documentation	Agencies MUST detail information security incident responsibilities and procedures for each system in the relevant Information Security Documents.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
7.3.6.C.01	Recording information security incidents	Agencies SHOULD ensure that all information security incidents are recorded in a register.	Functional	Intersects With	Situational Awareness For Incidents	IRO-09	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	
7.3.6.C.02	Recording information security incidents	Agencies SHOULD use their incidents register as a reference for future security risk assessments.	Functional	Intersects With	Situational Awareness For Incidents	IRO-09	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	
7.3.7.C.01	Handling data spills or data breach	Agencies MUST implement procedures and processes to detect data spills or data breach.	Functional	Intersects With	Sensitive / Regulated Data Spill Response	IRO-12	Mechanisms exist to respond to sensitive and/or regulated data spills.	5	
7.3.7.C.02	Handling data spills or data breach	When a data spill occurs agencies MUST assume that data at the highest classification held on or processed by the system, has been compromised.	Functional	Intersects With	Sensitive / Regulated Data Spill Response	IRO-12	Mechanisms exist to respond to sensitive and/or regulated data spills.	5	
7.3.7.C.03	Handling data spills or data breach	Agency SOPs MUST include procedure for: all personnel with access to systems; notification to the ITSM of any data spillage or breaches; and notification to the ITSM of access to any data which they are not authorised to access.	Functional	Intersects With	Sensitive / Regulated Data Spill Response	IRO-12	Mechanisms exist to respond to sensitive and/or regulated data spills.	5	
7.3.7.C.04	Handling data spills or data breach	Agencies MUST document procedures for dealing with data spills or data breaches in their IRP.	Functional	Intersects With	Sensitive / Regulated Data Spill Response	IRO-12	Mechanisms exist to respond to sensitive and/or regulated data spills.	5	
7.3.7.C.05	Handling data spills or data breach	Agencies MUST treat any data spill or data breach as an information security incident and follow the IRP to deal with it.	Functional	Intersects With	Sensitive / Regulated Data Spill Response	IRO-12	Mechanisms exist to respond to sensitive and/or regulated data spills.	5	
7.3.7.C.06	Handling data spills or data breach	When a data spill or data breach occurs agencies MUST report the details to the Privacy Commissioner and information owner in accordance with the Privacy Act 2020.	Functional	Intersects With	Sensitive / Regulated Data Spill Response	IRO-12	Mechanisms exist to respond to sensitive and/or regulated data spills.	5	
7.3.8.C.01	Containing data spills	When classified information is introduced onto a system not accredited to handle the information, the following actions MUST be followed: Immediately seek the advice of an ITSM; Segregate or isolate the affected system and/or data spill; Personnel MUST NOT delete the higher classified information unless specifically authorised by an ITSM.	Functional	Intersects With	Sensitive / Regulated Data Spill Response	IRO-12	Mechanisms exist to respond to sensitive and/or regulated data spills.	5	
7.3.8.C.01	Containing data spills	When classified information is introduced onto a system not accredited to handle the information, the following actions MUST be followed: Immediately seek the advice of an ITSM; Segregate or isolate the affected system and/or data spill; Personnel MUST NOT delete the higher classified information unless specifically authorised by an ITSM.	Functional	Intersects With	Sensitive / Regulated Data Exposure to Unauthorized Personnel	IRO-12.4	Mechanisms exist to address security safeguards for personnel exposed to sensitive and/or regulated data that is not within their assigned access authorizations.	5	
7.3.8.C.02	Containing data spills	When classified information is introduced onto a system not accredited to handle the information, personnel MUST NOT copy, view, print or email the information.	Functional	Intersects With	Sensitive / Regulated Data Spill Response	IRO-12	Mechanisms exist to respond to sensitive and/or regulated data spills.	5	
7.3.8.C.02	Containing data spills	When classified information is introduced onto a system not accredited to handle the information, personnel MUST NOT copy, view, print or email the information.	Functional	Intersects With	Sensitive / Regulated Data Exposure to Unauthorized Personnel	IRO-12.4	Mechanisms exist to address security safeguards for personnel exposed to sensitive and/or regulated data that is not within their assigned access authorizations.	5	
7.3.8.C.03	Containing data spills	When a data spill or data breach involving classified or sensitive information or contamination of classified systems occurs and systems cannot be segregated, or isolated agencies SHOULD immediately contact the NCSC for further advice.	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive and/or regulated data incidents in a timely manner.	5	
7.3.8.C.03	Containing data spills	When a data spill or data breach involving classified or sensitive information or contamination of classified systems occurs and systems cannot be segregated, or isolated agencies SHOULD immediately contact the NCSC for further advice.	Functional	Intersects With	Sensitive / Regulated Data Spill Response	IRO-12	Mechanisms exist to respond to sensitive and/or regulated data spills.	5	
7.3.9.C.01	Handling malicious code infection	Agencies SHOULD follow the steps described below when malicious code is detected: isolate the infected system; decide whether to request assistance from NCSC; if such assistance is requested and agreed to, delay any further action until advised by NCSC; check connected systems and media including backups for malicious code; isolate all infected systems and media to prevent reinfection; change all passwords and key material stored or potentially accessed from compromised systems, including any websites with password controlled access; advise system users of any relevant aspects of the compromise, including a recommendation to change all passwords on compromised systems; revoke all session tokens associated with user and/or device; use up-to-date anti-malware software to remove the malware from the systems or media; monitor network traffic for malicious activity; record and report the information security incident and perform any other activities specified in the IRP; and in certain scenarios rebuilding and reinitialising the system and/or user profile may be required.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
7.3.9.C.01	Handling malicious code infection	Agencies SHOULD follow the steps described below when malicious code is detected: isolate the infected system; decide whether to request assistance from NCSC; if such assistance is requested and agreed to, delay any further action until advised by NCSC; check connected systems and media including backups for malicious code; isolate all infected systems and media to prevent reinfection; change all passwords and key material stored or potentially accessed from compromised systems, including any websites with password controlled access; advise system users of any relevant aspects of the compromise, including a recommendation to change all passwords on compromised systems; revoke all session tokens associated with user and/or device; use up-to-date anti-malware software to remove the malware from the systems or media; monitor network traffic for malicious activity; record and report the information security incident and perform any other activities specified in the IRP; and in certain scenarios rebuilding and reinitialising the system and/or user profile may be required.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
7.3.10.C.01	Allowing continued attacks	Agencies considering allowing an attacker to continue some actions under controlled conditions for the purpose of seeking further information or evidence MUST seek legal advice.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
7.3.10.C.01	Allowing continued attacks	Agencies considering allowing an attacker to continue some actions under controlled conditions for the purpose of seeking further information or evidence MUST seek legal advice.	Functional	Intersects With	Correlation with External Organizations	IRO-02.5	Mechanisms exist to coordinate with approved third-parties to achieve a cross-organization perspective on incident awareness and more effective incident responses.	5	
7.3.10.C.01	Allowing continued attacks	Agencies considering allowing an attacker to continue some actions under controlled conditions for the purpose of seeking further information or evidence MUST seek legal advice.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
7.3.10.C.01	Allowing continued attacks	Agencies considering allowing an attacker to continue some actions under controlled conditions for the purpose of seeking further information or evidence MUST seek legal advice.	Functional	Intersects With	Coordination With External Providers	IRO-11.2	Mechanisms exist to establish a direct, cooperative relationship between the organization's incident response capability and external service providers.	5	
7.3.11.C.01	Integrity of evidence	Agencies SHOULD: transfer a copy of raw audit trails and other relevant data onto media for secure archiving, as well as securing manual log records for retention; and ensure that all personnel involved in the investigation maintain a record of actions undertaken to support the investigation.	Functional	Intersects With	Chain of Custody & Forensics	IRO-08	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	5	
7.3.11.C.01	Integrity of evidence	Agencies SHOULD: transfer a copy of raw audit trails and other relevant data onto media for secure archiving, as well as securing manual log records for retention; and ensure that all personnel involved in the investigation maintain a record of actions undertaken to support the investigation.	Functional	Intersects With	Coordination With External Providers	IRO-11.2	Mechanisms exist to establish a direct, cooperative relationship between the organization's incident response capability and external service providers.	5	
7.3.12.C.01	Seeking assistance	Agencies SHOULD ensure that any requests for NCSC assistance are made as soon as possible after the information security incident is detected and that no actions which could affect the integrity of the evidence are carried out prior to NCSCs involvement.	Functional	Intersects With	Incident Reporting Assistance	IRO-11	Mechanisms exist to provide incident response advice and assistance to users of Technology Assets, Applications and/or Services (TAAS) for the handling and reporting of actual and potential cybersecurity and data protection incidents.	5	
7.3.12.C.01	Seeking assistance	Agencies SHOULD ensure that any requests for NCSC assistance are made as soon as possible after the information security incident is detected and that no actions which could affect the integrity of the evidence are carried out prior to NCSCs involvement.	Functional	Intersects With	Coordination With External Providers	IRO-11.2	Mechanisms exist to establish a direct, cooperative relationship between the organization's incident response capability and external service providers.	5	
8.1.10.C.01	Facility physical security	Agencies MUST ensure that any facility containing a system or its associated infrastructure, including deployable systems, are certified and accredited in accordance with the PSR.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
8.1.11.C.01	Preventing observation by unauthorised people	Agencies SHOULD prevent unauthorised people from observing systems, in particular desks, screens and keyboards.	Functional	Intersects With	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	5	
8.1.11.C.02	Preventing observation by unauthorised people	Agencies SHOULD position desks, screens and keyboards away from windows and doorways so that they cannot be overseen by unauthorised persons. If required, blinds or drapes SHOULD be fixed to the inside of windows, and doors kept closed to avoid oversight.	Functional	Intersects With	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	5	
8.1.12.C.01	Bringing non-agency owned devices into secure areas	Agencies MUST NOT permit non-agency owned devices to be brought into TOP SECRET areas without prior approval from the Accreditation Authority.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
8.1.12.C.01	Bringing non-agency owned devices into secure areas	Agencies MUST NOT permit non-agency owned devices to be brought into TOP SECRET areas without prior approval from the Accreditation Authority.	Functional	Intersects With	Terms of Employment	HRS-05	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	
8.1.12.C.01	Bringing non-agency owned devices into secure areas	Agencies MUST NOT permit non-agency owned devices to be brought into TOP SECRET areas without prior approval from the Accreditation Authority.	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	
8.1.12.C.01	Bringing non-agency owned devices into secure areas	Agencies MUST NOT permit non-agency owned devices to be brought into TOP SECRET areas without prior approval from the Accreditation Authority.	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
8.1.12.C.01	Bringing non-agency owned devices into secure areas	Agencies MUST NOT permit non-agency owned devices to be brought into TOP SECRET areas without prior approval from the Accreditation Authority.	Functional	Intersects With	Searches	PES-04.2	Physical access control mechanisms exist to inspect personnel and their personal effects (e.g., personal property ordinarily worn or carried by the individual, including vehicles) to prevent the unauthorized exfiltration of data and technology assets.	5	
8.1.13.C.01	Technical Inspection and surveillance counter-measure testing	Agencies MUST ensure that technical surveillance counter-measure tests are conducted as a part of the physical security certification.	Functional	Intersects With	Searches	PES-04.2	Physical access control mechanisms exist to inspect personnel and their personal effects (e.g., personal property ordinarily worn or carried by the individual, including vehicles) to prevent the unauthorized exfiltration of data and technology assets.	5	
8.1.13.C.01	Technical Inspection and surveillance counter-measure testing	Agencies MUST ensure that technical surveillance counter-measure tests are conducted as a part of the physical security certification.	Functional	Intersects With	Technical Surveillance Countermeasures Security	VPM-08	Mechanisms exist to utilize a technical surveillance countermeasures survey.	5	
8.1.13.C.02	Technical Inspection and surveillance counter-measure testing	Agencies MUST determine if further technical surveillance counter-measure testing is required, particularly if visitors or contractors have entered secure areas.	Functional	Intersects With	Searches	PES-04.2	Physical access control mechanisms exist to inspect personnel and their personal effects (e.g., personal property ordinarily worn or carried by the individual, including vehicles) to prevent the unauthorized exfiltration of data and technology assets.	5	
8.1.13.C.02	Technical Inspection and surveillance counter-measure testing	Agencies MUST determine if further technical surveillance counter-measure testing is required, particularly if visitors or contractors have entered secure areas.	Functional	Intersects With	Technical Surveillance Countermeasures Security	VPM-08	Mechanisms exist to utilize a technical surveillance countermeasures survey.	5	
8.2.5.C.01	Securing servers and network devices	Agencies MUST ensure that servers and network devices are secured within cabinets as outlined in PSR Policy Framework - Physical security and supporting documentation.	Functional	Intersects With	Lockable Physical Casings	PES-03.2	Physical access control mechanisms exist to protect system components from unauthorized physical access (e.g., lockable physical casings).	5	
8.2.6.C.01	Securing server rooms, communications rooms and security containers	Agencies MUST ensure that keys or equivalent access mechanisms to server rooms, communications rooms and security containers are appropriately controlled.	Functional	Intersects With	Physical Security of Offices, Rooms & Facilities	PES-04	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	5	
8.2.6.C.02	Securing server rooms, communications rooms and security containers	Agencies MUST NOT leave server rooms, communications rooms or security containers in an unsecured state unless the server room is occupied by authorised personnel.	Functional	Intersects With	Physical Security of Offices, Rooms & Facilities	PES-04	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	5	
8.2.7.C.01	Administrative measures - Site security plans	Agencies MUST develop a Site Security Plan (SitePlan) for each server and communications room. Information to be covered includes, but is not limited to: a summary of the security risk review for the facility the server or communications room is located in; roles and responsibilities of facility and security personnel; the administration, operation and maintenance of the electronic access control system or security alarm system; key management, the enrolment and removal of system users and issuing of personal identification number codes and passwords; personnel security clearances, security awareness training and regular briefings; regular inspection of the generated audit trails and logs; end of day checks and lockup; reporting of information security incidents; and what activities to undertake in response to security alarms.	Functional	Intersects With	Physical Security Plan (PSP)	PES-01.1	Mechanisms exist to document a Physical Security Plan (PSP), or similar document, to summarize the implemented security controls to protect physical access to technology assets, as well as applicable risks and threats.	5	
8.2.8.C.01	No-lone-zones	Agencies operating no-lone-zones MUST suitably signpost the area and have all entry and exit points appropriately secured.	Functional	Intersects With	Dual Authorization for Physical Access	PES-02.2	Mechanisms exist to enforce a "two-person rule" for physical access by requiring two authorized individuals with separate access cards, keys or PINs, to access highly-sensitive areas (e.g., safe, high-security cage, etc.).	5	
8.3.3.C.01	Network infrastructure in secure areas	Agencies MUST certify the physical security of facilities containing network infrastructure to the highest classification of information being communicated over the network infrastructure.	Functional	Intersects With	Access To Critical Systems	PES-03.4	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	
8.3.3.C.01	Network infrastructure in secure areas	Agencies MUST certify the physical security of facilities containing network infrastructure to the highest classification of information being communicated over the network infrastructure.	Functional	Intersects With	Supporting Utilities	PES-07	Facility security mechanisms exist to protect power equipment and power cabling for the system from damage and destruction.	5	
8.3.3.C.01	Network infrastructure in secure areas	Agencies MUST certify the physical security of facilities containing network infrastructure to the highest classification of information being communicated over the network infrastructure.	Functional	Intersects With	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	5	
8.3.3.C.01	Network infrastructure in secure areas	Agencies MUST certify the physical security of facilities containing network infrastructure to the highest classification of information being communicated over the network infrastructure.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
8.3.3.C.02	Network infrastructure in secure areas	Agencies communicating classified information over infrastructure in secure areas SHOULD encrypt their information with at least an Approved Cryptographic Protocol. See Section 17.3 - Approved Cryptographic Protocols.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
8.3.4.C.01	Protecting network infrastructure	Agencies MUST locate patch panels, fibre distribution panels and structured wiring enclosures within at least lockable commercial cabinets.	Functional	Intersects With	Access To Critical Systems	PES-03.4	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	
8.3.4.C.01	Protecting network infrastructure	Agencies MUST locate patch panels, fibre distribution panels and structured wiring enclosures within at least lockable commercial cabinets.	Functional	Intersects With	Supporting Utilities	PES-07	Facility security mechanisms exist to protect power equipment and power cabling for the system from damage and destruction.	5	
8.3.4.C.01	Protecting network infrastructure	Agencies MUST locate patch panels, fibre distribution panels and structured wiring enclosures within at least lockable commercial cabinets.	Functional	Intersects With	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	5	
8.3.4.C.01	Protecting network infrastructure	Agencies MUST locate patch panels, fibre distribution panels and structured wiring enclosures within at least lockable commercial cabinets.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
8.3.4.C.02	Protecting network infrastructure	Agencies SHOULD locate patch panels, fibre distribution panels and structured wiring enclosures within at least lockable commercial cabinets.	Functional	Intersects With	Access To Critical Systems	PES-03.4	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	
8.3.4.C.02	Protecting network infrastructure	Agencies SHOULD locate patch panels, fibre distribution panels and structured wiring enclosures within at least lockable commercial cabinets.	Functional	Intersects With	Supporting Utilities	PES-07	Facility security mechanisms exist to protect power equipment and power cabling for the system from damage and destruction.	5	
8.3.4.C.02	Protecting network infrastructure	Agencies SHOULD locate patch panels, fibre distribution panels and structured wiring enclosures within at least lockable commercial cabinets.	Functional	Intersects With	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	5	
8.3.4.C.02	Protecting network infrastructure	Agencies SHOULD locate patch panels, fibre distribution panels and structured wiring enclosures within at least lockable commercial cabinets.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
8.3.5.C.01	Network infrastructure in unsecure areas	Agencies communicating classified information over public network infrastructure or over infrastructure in unsecure areas MUST use encryption to lower the handling instructions to be equivalent to those for unclassified networks.	Functional	Intersects With	Access To Critical Systems	PES-03.4	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	
8.3.5.C.01	Network infrastructure in unsecure areas	Agencies communicating classified information over public network infrastructure or over infrastructure in unsecure areas MUST use encryption to lower the handling instructions to be equivalent to those for unclassified networks.	Functional	Intersects With	Supporting Utilities	PES-07	Facility security mechanisms exist to protect power equipment and power cabling for the system from damage and destruction.	5	
8.3.5.C.01	Network infrastructure in unsecure areas	Agencies communicating classified information over public network infrastructure or over infrastructure in unsecure areas MUST use encryption to lower the handling instructions to be equivalent to those for unclassified networks.	Functional	Intersects With	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	5	
8.3.5.C.01	Network infrastructure in unsecure areas	Agencies communicating classified information over public network infrastructure or over infrastructure in unsecure areas MUST use encryption to lower the handling instructions to be equivalent to those for unclassified networks.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
8.4.8.C.01	Accounting for IT equipment	Agencies MUST account for all IT equipment containing media.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5	
8.4.9.C.01	Processing requirements	Agencies MUST certify the physical security of facilities containing IT equipment to the highest classification of information being processed, stored or communicated by the equipment within the facilities.	Functional	Subset Of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
8.4.9.C.01	Processing requirements	Agencies MUST certify the physical security of facilities containing IT equipment to the highest classification of information being processed, stored or communicated by the equipment within the facilities.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5	
8.4.10.C.01	Storage requirements	Agencies MUST ensure that when secure areas are non-operational or when work areas are unoccupied IT equipment with media is secured in accordance with the minimum physical security requirements for storing classified information as specified in the PSR Policy Framework - Physical security and supporting documents.	Functional	Intersects With	Media Storage	DCH-06	Mechanisms exist to: (1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and (2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures.	5	
8.4.11.C.01	Securing non-volatile media for storage	Agencies choosing to prevent the storage of classified information on non-volatile media and enforcing scrubbing of temporary data at logoff or shutdown SHOULD: assess the security risks associated with such a decision; and specify the processes and conditions for their application within the systems SSP.	Functional	Intersects With	Media Storage	DCH-06	Mechanisms exist to: (1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and (2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures.	5	
8.4.12.C.01	Securing volatile media for storage	Agencies securing volatile media for IT equipment during non-operational hours SHOULD: disconnect power from the equipment the media resides within; assess the security risks if not sanitising the media; and specify any additional processes and controls that will be applied within the systems SSP.	Functional	Intersects With	Media Storage	DCH-06	Mechanisms exist to: (1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and (2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures.	5	
8.4.13.C.01	Encrypting media within IT equipment	Agencies SHOULD encrypt media within IT equipment with an Approved Cryptographic Algorithm. See Section 17.2 - Approved Cryptographic Algorithms.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
8.4.13.C.01	Encrypting media within IT equipment	Agencies SHOULD encrypt media within IT equipment with an Approved Cryptographic Algorithm. See Section 17.2 - Approved Cryptographic Algorithms.	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
8.4.13.C.01	Encrypting media within IT equipment	Agencies SHOULD encrypt media within IT equipment with an Approved Cryptographic Algorithm. See Section 17.2 - Approved Cryptographic Algorithms.	Functional	Intersects With	Storage Media	CRY-05.1	Cryptographic mechanisms exist to protect the confidentiality and integrity of sensitive and/or regulated data residing on storage media.	5	
8.4.13.C.01	Encrypting media within IT equipment	Agencies SHOULD encrypt media within IT equipment with an Approved Cryptographic Algorithm. See Section 17.2 - Approved Cryptographic Algorithms.	Functional	Intersects With	Media Storage	DCH-06	Mechanisms exist to: (1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and (2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures.	5	
8.4.13.C.01	Encrypting media within IT equipment	Agencies SHOULD encrypt media within IT equipment with an Approved Cryptographic Algorithm. See Section 17.2 - Approved Cryptographic Algorithms.	Functional	Intersects With	Making Sensitive Data Unreadable In Storage	DCH-06.4	Mechanisms exist to ensure sensitive and/or regulated data is rendered human unreadable anywhere sensitive and/or regulated data is stored.	5	
8.4.13.C.01	Encrypting media within IT equipment	Agencies SHOULD encrypt media within IT equipment with an Approved Cryptographic Algorithm. See Section 17.2 - Approved Cryptographic Algorithms.	Functional	Intersects With	Encrypting Data In Storage Media	DCH-07.2	Cryptographic mechanisms exist to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	5	
8.5.3.C.01	Recording seal usage	Agencies MUST record the usage of seals in a register that is appropriately secured.	Functional	Intersects With	Physical Tampering Detection	AST-08	Mechanisms exist to periodically inspect systems and system components for Indicators of Compromise (IoC).	5	
8.5.3.C.02	Recording seal usage	Agencies MUST record in a register, information on: issue and usage details of seals and associated tools; serial numbers of all seals purchased; and the location or asset on which each seal is used.	Functional	Intersects With	Physical Tampering Detection	AST-08	Mechanisms exist to periodically inspect systems and system components for Indicators of Compromise (IoC).	5	
8.5.3.C.03	Recording seal usage	Agencies SHOULD record the usage of seals in a register that is appropriately secured.	Functional	Intersects With	Physical Tampering Detection	AST-08	Mechanisms exist to periodically inspect systems and system components for Indicators of Compromise (IoC).	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
8.5.3.C.04	Recording seal usage	Agencies SHOULD record in a register information on: issue and usage details of seals and associated tools; serial numbers of all seals purchased; and the location or asset on which each seal is used.	Functional	Intersects With	Physical Tampering Detection	AST-08	Mechanisms exist to periodically inspect systems and system components for Indicators of Compromise (IoC).	5	
8.5.4.C.01	Purchasing seals	Agencies SHOULD consult with the seal manufacturer to ensure that, if available, any purchased seals and sealing tools display a unique identifier or image appropriate to the agency.	Functional	Intersects With	Physical Tampering Detection	AST-08	Mechanisms exist to periodically inspect systems and system components for Indicators of Compromise (IoC).	5	
8.5.4.C.02	Purchasing seals	Seals and any seal application tools SHOULD be secured when not in use.	Functional	Intersects With	Physical Tampering Detection	AST-08	Mechanisms exist to periodically inspect systems and system components for Indicators of Compromise (IoC).	5	
8.5.4.C.03	Purchasing seals	Agencies SHOULD NOT allow contractors to independently purchase seals and associated tools on behalf of the government.	Functional	Intersects With	Physical Tampering Detection	AST-08	Mechanisms exist to periodically inspect systems and system components for Indicators of Compromise (IoC).	5	
8.5.5.C.01	Reviewing seal usage	Agencies SHOULD review seals for differences with a register at least annually. At the same time seals SHOULD be examined for any evidence of tampering.	Functional	Intersects With	Physical Tampering Detection	AST-08	Mechanisms exist to periodically inspect systems and system components for Indicators of Compromise (IoC).	5	
9.1.4.C.01	Information security awareness and training responsibility	Agency management MUST ensure that all personnel who have access to a system have sufficient training and ongoing information security awareness.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
9.1.5.C.01	Information security awareness and training	Agencies MUST provide ongoing information security awareness and a training programme for personnel on topics such as responsibilities, legislation and regulation, consequences of non-compliance with information security policies and procedures, and potential security risks and counter-measures.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	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	
9.1.5.C.02	Information security awareness and training	Agencies MUST provide information security awareness training as part of their employee induction programmes.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	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	
9.1.6.C.01	Degree and content of information security awareness and training	Agencies SHOULD align the detail, content and coverage of information security awareness and training programmes to system user responsibilities.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	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	
9.1.6.C.01	Degree and content of information security awareness and training	Agencies SHOULD align the detail, content and coverage of information security awareness and training programmes to system user responsibilities.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	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	
9.1.6.C.02	Degree and content of information security awareness and training	Agencies SHOULD ensure that information security awareness and training includes information on: the purpose of the training or awareness program; any legislative or regulatory mandates and requirements; any national or agency policy mandates and requirements; agency security appointments and contacts; the legitimate use of system accounts, software and classified information; the security of accounts, including shared passwords; authorisation requirements for applications, databases and data; the security risks associated with non-agency systems, particularly the Internet; reporting any suspected compromises or anomalies; reporting requirements for information security incidents, suspected compromises or anomalies; classifying, marking, controlling, storing and sanitising media; protecting workstations from unauthorised access; informing the support section when access to a system is no longer needed; observing rules and regulations governing the secure operation and authorised use of systems; and supporting documentation such as SOPs and user guides.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	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	
9.1.6.C.02	Degree and content of information security awareness and training	Agencies SHOULD ensure that information security awareness and training includes information on: the purpose of the training or awareness program; any legislative or regulatory mandates and requirements; any national or agency policy mandates and requirements; agency security appointments and contacts; the legitimate use of system accounts, software and classified information; the security of accounts, including shared passwords; authorisation requirements for applications, databases and data; the security risks associated with non-agency systems, particularly the Internet; reporting any suspected compromises or anomalies; reporting requirements for information security incidents, suspected compromises or anomalies; classifying, marking, controlling, storing and sanitising media; protecting workstations from unauthorised access; informing the support section when access to a system is no longer needed; observing rules and regulations governing the secure operation and authorised use of systems; and supporting documentation such as SOPs and user guides.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	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	
9.1.6.C.03	Degree and content of information security awareness and training	Agencies SHOULD ensure that information security awareness and training includes advice to system users not to attempt to: tamper with the system; bypass, strain or test information security mechanisms; introduce or use unauthorised IT equipment or software on a system; replace items such as keyboards, pointing devices and other peripherals with personal equipment; assume the roles and privileges of others; attempt to gain access to classified information for which they have no authorisation; or relocate equipment without proper authorisation.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	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	
9.1.7.C.01	System familiarisation training	Agencies MUST provide all system users with familiarisation training on the information security policies and procedures and the secure operation of the system before being granted unsupervised access to the system.	Functional	Intersects With	Formal Indoctrination	HRS-04.2	Mechanisms exist to formally educate authorized users on proper data handling practices for all the relevant types of data to which they have access.	5	
9.1.8.C.01	Disclosure of information while on courses	Agencies SHOULD advise personnel attending courses along with non-government personnel not to disclose any details that could be used to compromise agency security.	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	
9.1.8.C.01	Disclosure of information while on courses	Agencies SHOULD advise personnel attending courses along with non-government personnel not to disclose any details that could be used to compromise agency security.	Functional	Intersects With	Confidentiality Agreements	HRS-06.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, or both employees and third-parties.	5	
9.2.10.C.01	Documenting authorisations, security clearance and briefing requirements	Agencies MUST specify in the System Security Plan (SSP) any authorisations, security clearances and briefings necessary for system access.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
9.2.10.C.01	Documenting authorisations, security clearance and briefing requirements	Agencies MUST specify in the System Security Plan (SSP) any authorisations, security clearances and briefings necessary for system access.	Functional	Intersects With	Position Categorization	HRS-02	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	
9.2.10.C.01	Documenting authorisations, security clearance and briefing requirements	Agencies MUST specify in the System Security Plan (SSP) any authorisations, security clearances and briefings necessary for system access.	Functional	Intersects With	Citizenship Requirements	HRS-04.3	Mechanisms exist to verify that individuals accessing a system processing, storing, or transmitting sensitive information meet applicable statutory, regulatory and/or contractual requirements for citizenship.	5	
9.2.11.C.01	Authorisation and system access	Agencies MUST: limit system access on a need-to-know/need-to-access basis; provide system users with the least amount of privileges needed to undertake their duties; and have any requests for access to a system authorised by the supervisor or manager of the system user.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
9.2.11.C.01	Authorisation and system access	Agencies MUST: limit system access on a need-to-know/need-to-access basis; provide system users with the least amount of privileges needed to undertake their duties; and have any requests for access to a system authorised by the supervisor or manager of the system user.	Functional	Intersects With	Position Categorization	HRS-02	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	
9.2.11.C.01	Authorisation and system access	Agencies MUST: limit system access on a need-to-know/need-to-access basis; provide system users with the least amount of privileges needed to undertake their duties; and have any requests for access to a system authorised by the supervisor or manager of the system user.	Functional	Intersects With	Citizenship Requirements	HRS-04.3	Mechanisms exist to verify that individuals accessing a system processing, storing, or transmitting sensitive information meet applicable statutory, regulatory and/or contractual requirements for citizenship.	5	
9.2.11.C.01	Authorisation and system access	Agencies MUST: limit system access on a need-to-know/need-to-access basis; provide system users with the least amount of privileges needed to undertake their duties; and have any requests for access to a system authorised by the supervisor or manager of the system user.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5	
9.2.11.C.02	Authorisation and system access	Agencies SHOULD: limit system access on a need-to-know/need-to-access basis; provide system users with the least amount of privileges needed to undertake their duties; have any requests for access to a system authorised by the supervisor or manager of the system user; and ensure a formal acknowledgement of the security briefing is obtained and recorded.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
9.2.11.C.02	Authorisation and system access	Agencies SHOULD: limit system access on a need-to-know/need-to-access basis; provide system users with the least amount of privileges needed to undertake their duties; have any requests for access to a system authorised by the supervisor or manager of the system user; and ensure a formal acknowledgement of the security briefing is obtained and recorded.	Functional	Intersects With	Position Categorization	HRS-02	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	
9.2.11.C.02	Authorisation and system access	Agencies SHOULD: limit system access on a need-to-know/need-to-access basis; provide system users with the least amount of privileges needed to undertake their duties; have any requests for access to a system authorised by the supervisor or manager of the system user; and ensure a formal acknowledgement of the security briefing is obtained and recorded.	Functional	Intersects With	Citizenship Requirements	HRS-04.3	Mechanisms exist to verify that individuals accessing a system processing, storing, or transmitting sensitive information meet applicable statutory, regulatory and/or contractual requirements for citizenship.	5	
9.2.11.C.02	Authorisation and system access	Agencies SHOULD: limit system access on a need-to-know/need-to-access basis; provide system users with the least amount of privileges needed to undertake their duties; have any requests for access to a system authorised by the supervisor or manager of the system user; and ensure a formal acknowledgement of the security briefing is obtained and recorded.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5	
9.2.12.C.01	Recording authorisation for personnel to access systems	Agencies SHOULD: maintain a secure record of: all authorised system users; their user identification; why access is required; role and privilege level, who provided the authorisation to access the system; when the authorisation was granted; and keep a copy of the acknowledgement signed by the individual granted a clearance; and maintain the record, for the life of the system or information to which access is granted, or the length of employment, whichever is the longer.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
9.2.13.C.01	Security clearance for system access	System users MUST NOT be granted access to systems or information classified CONFIDENTIAL or above unless vetting procedures have been completed and formal security clearance granted.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
9.2.13.C.02	Security clearance for system access	All system users MUST: hold a security clearance or other authorisation appropriate for the system classification; or have been granted access in accordance with the requirements in the PSR for emergency access.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
9.2.14.C.01	System access briefings	All system users MUST have received any necessary briefings before being granted access to compartmented or endorsed information or systems.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
9.2.15.C.01	Access by foreign nationals to NZEO systems	Where systems process, store or communicate unprotected NZEO information, agencies MUST NOT allow foreign nationals, including seconded foreign nationals, to have access to the system.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
9.2.15.C.01	Access by foreign nationals to NZEO systems	Where systems process, store or communicate unprotected NZEO information, agencies MUST NOT allow foreign nationals, including seconded foreign nationals, to have access to the system.	Functional	Intersects With	Citizenship Requirements	HRS-04.3	Mechanisms exist to verify that individuals accessing a system processing, storing, or transmitting sensitive information meet applicable statutory, regulatory and/or contractual requirements for citizenship.	5	
9.2.15.C.01	Access by foreign nationals to NZEO systems	Where systems process, store or communicate unprotected NZEO information, agencies MUST NOT allow foreign nationals, including seconded foreign nationals, to have access to the system.	Functional	Intersects With	Citizenship Identification	HRS-04.4	Mechanisms exist to identify foreign nationals, including by their specific citizenship.	5	
9.2.15.C.02	Access by foreign nationals to NZEO systems	Where agencies protect NZEO information on a system by implementing controls to ensure that NZEO information is not passed to, or made accessible to, foreign nationals, agencies MUST NOT allow foreign nationals, including seconded foreign nationals, to have access to the system.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
9.2.15.C.02	Access by foreign nationals to NZEO systems	Where agencies protect NZEO information on a system by implementing controls to ensure that NZEO information is not passed to, or made accessible to, foreign nationals, agencies MUST NOT allow foreign nationals, including seconded foreign nationals, to have access to the system.	Functional	Intersects With	Citizenship Requirements	HRS-04.3	Mechanisms exist to verify that individuals accessing a system processing, storing, or transmitting sensitive information meet applicable statutory, regulatory and/or contractual requirements for citizenship.	5	
9.2.15.C.02	Access by foreign nationals to NZEO systems	Where agencies protect NZEO information on a system by implementing controls to ensure that NZEO information is not passed to, or made accessible to, foreign nationals, agencies MUST NOT allow foreign nationals, including seconded foreign nationals, to have access to the system.	Functional	Intersects With	Citizenship Identification	HRS-04.4	Mechanisms exist to identify foreign nationals, including by their specific citizenship.	5	
9.2.16.C.01	Access by foreign nationals to New Zealand systems	Where systems process, store or communicate classified information with nationality releasability markings, agencies MUST NOT allow foreign nationals, including seconded foreign nationals, to have access to such information that is not marked as releasable to their nation.	Functional	Intersects With	Citizenship Requirements	HRS-04.3	Mechanisms exist to verify that individuals accessing a system processing, storing, or transmitting sensitive information meet applicable statutory, regulatory and/or contractual requirements for citizenship.	5	
9.2.16.C.01	Access by foreign nationals to New Zealand systems	Where systems process, store or communicate classified information with nationality releasability markings, agencies MUST NOT allow foreign nationals, including seconded foreign nationals, to have access to such information that is not marked as releasable to their nation.	Functional	Intersects With	Citizenship Identification	HRS-04.4	Mechanisms exist to identify foreign nationals, including by their specific citizenship.	5	
9.2.17.C.01	Granting limited higher access	Agencies MUST NOT permit limited higher access for systems and information classified CONFIDENTIAL or above.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
9.2.17.C.02	Granting limited higher access	Agencies granting limited higher access to information or systems MUST ensure that: the requirement to grant limited higher access is temporary in nature and is an exception rather than the norm; an ITSM has recommended the limited higher access; a cessation date for limited higher access has been set; the access period does not exceed two months; the limited higher access is granted on an occasional NOT non-ongoing basis; the system user is not granted privileged access to the system; the system users access is formally documented; and the system users access is approved by the CISO.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
9.2.18.C.01	Controlling limited higher access	Agencies granting limited higher access to a system MUST ensure that: the approval for access is formally acknowledged and recorded; and either effective controls are in place to restrict access only to classified information that is necessary to undertake the system users duties; or the system user is continually supervised by another system user who has the appropriate security clearances to access the system.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
9.2.19.C.01	Granting emergency access	Emergency access MUST NOT be granted unless personnel have a security clearance to at least CONFIDENTIAL level.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
9.2.19.C.02	Granting emergency access	Emergency access MUST NOT be used on reassignment of duties while awaiting completion of full security clearance procedures.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
9.2.19.C.03	Granting emergency access	Agencies granting emergency access to a system MUST ensure that: the requirements to grant emergency access is due to an immediate and critical need to access classified information and there is insufficient time to complete clearance procedures; the agency head or their delegate has approved the emergency access; the system users access is formally documented; the system users access is reported to the CISO; appropriate briefs and debriefs for the information and system are conducted; access is limited to information and systems necessary to deal with the particular emergency and is governed by strict application of the "need to know" principle; emergency access is limited to ONE security clearance level higher than the clearance currently held; and the security clearance process is completed as soon as possible.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
9.2.19.C.04	Granting emergency access	Personnel granted emergency access MUST be debriefed at the conclusion of the emergency.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
9.2.20.C.01	Accessing endorsed or compartmented information	Agencies MUST NOT grant limited higher access to systems that process, store or communicate endorsed or compartmented information.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
9.3.4.C.01	Using the Internet	Agencies MUST ensure personnel are instructed to report any suspicious activity, questioning or contact when using the Internet, to an ITSM.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	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	
9.3.5.C.01	Awareness of Web usage policies	Agencies MUST make their system users aware of the agency's Web usage policies.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	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	
9.3.5.C.02	Awareness of Web usage policies	Personnel MUST formally acknowledge and accept agency Web usage policies.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	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	
9.3.6.C.01	Monitoring Web usage	Agencies SHOULD implement measures to monitor their personnel, visitor and contractor compliance with their Web usage policies.	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
9.3.7.C.01	Posting information on the Web	Agencies MUST ensure personnel are instructed to take special care when posting information on the Web.	Functional	Intersects With	Terms of Employment	HRS-05	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	
9.3.7.C.01	Posting information on the Web	Agencies MUST ensure personnel are instructed to take special care when posting information on the Web.	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	
9.3.7.C.01	Posting information on the Web	Agencies MUST ensure personnel are instructed to take special care when posting information on the Web.	Functional	Intersects With	Social Media & Social Networking Restrictions	HRS-05.2	Mechanisms exist to define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information.	5	
9.3.7.C.02	Posting information on the Web	Agencies MUST ensure personnel posting information on the Web maintain separate professional accounts from any personal accounts they have for websites.	Functional	Intersects With	Terms of Employment	HRS-05	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	
9.3.7.C.02	Posting information on the Web	Agencies MUST ensure personnel posting information on the Web maintain separate professional accounts from any personal accounts they have for websites.	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	
9.3.7.C.02	Posting information on the Web	Agencies MUST ensure personnel posting information on the Web maintain separate professional accounts from any personal accounts they have for websites.	Functional	Intersects With	Social Media & Social Networking Restrictions	HRS-05.2	Mechanisms exist to define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information.	5	
9.3.7.C.03	Posting information on the Web	Agencies SHOULD monitor websites where personnel post information and if necessary remove or request the removal of any inappropriate information.	Functional	Intersects With	Terms of Employment	HRS-05	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	
9.3.7.C.03	Posting information on the Web	Agencies SHOULD monitor websites where personnel post information and if necessary remove or request the removal of any inappropriate information.	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	
9.3.7.C.03	Posting information on the Web	Agencies SHOULD monitor websites where personnel post information and if necessary remove or request the removal of any inappropriate information.	Functional	Intersects With	Social Media & Social Networking Restrictions	HRS-05.2	Mechanisms exist to define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information.	5	
9.3.7.C.04	Posting information on the Web	Accessing personal accounts from agency systems SHOULD be discouraged.	Functional	Intersects With	Terms of Employment	HRS-05	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	
9.3.7.C.04	Posting information on the Web	Accessing personal accounts from agency systems SHOULD be discouraged.	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	
9.3.7.C.04	Posting information on the Web	Accessing personal accounts from agency systems SHOULD be discouraged.	Functional	Intersects With	Social Media & Social Networking Restrictions	HRS-05.2	Mechanisms exist to define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information.	5	
9.3.8.C.01	Posting personal information on the Web	Agencies SHOULD ensure that personnel are informed of the security risks associated with posting personal information on websites, especially for those personnel holding higher level security clearances.	Functional	Intersects With	Terms of Employment	HRS-05	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	
9.3.8.C.01	Posting personal information on the Web	Agencies SHOULD ensure that personnel are informed of the security risks associated with posting personal information on websites, especially for those personnel holding higher level security clearances.	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	
9.3.8.C.01	Posting personal information on the Web	Agencies SHOULD ensure that personnel are informed of the security risks associated with posting personal information on websites, especially for those personnel holding higher level security clearances.	Functional	Intersects With	Social Media & Social Networking Restrictions	HRS-05.2	Mechanisms exist to define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information.	5	
9.3.8.C.02	Posting personal information on the Web	Personnel SHOULD be encouraged to use privacy settings for websites to restrict access to personal information they post to only those they authorise to view it.	Functional	Intersects With	Terms of Employment	HRS-05	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	
9.3.8.C.02	Posting personal information on the Web	Personnel SHOULD be encouraged to use privacy settings for websites to restrict access to personal information they post to only those they authorise to view it.	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	
9.3.8.C.02	Posting personal information on the Web	Personnel SHOULD be encouraged to use privacy settings for websites to restrict access to personal information they post to only those they authorise to view it.	Functional	Intersects With	Social Media & Social Networking Restrictions	HRS-05.2	Mechanisms exist to define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information.	5	
9.3.8.C.03	Posting personal information on the Web	Personnel SHOULD be encouraged to undertake a Web search of themselves to determine what personal information is available and contact an ITSM if they need assistance in determining if the information is appropriate to be viewed by the general public or potential adversaries.	Functional	Intersects With	Terms of Employment	HRS-05	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	
9.3.8.C.03	Posting personal information on the Web	Personnel SHOULD be encouraged to undertake a Web search of themselves to determine what personal information is available and contact an ITSM if they need assistance in determining if the information is appropriate to be viewed by the general public or potential adversaries.	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
9.3.8.C.03	Posting personal information on the Web	Personnel SHOULD be encouraged to undertake a Web search of themselves to determine what personal information is available and contact an ITSM if they need assistance in determining if the information is appropriate to be viewed by the general public or potential adversaries.	Functional	Intersects With	Social Media & Social Networking Restrictions	HRS-05.2	Mechanisms exist to define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information.	5	
9.3.9.C.01	Peer-to-peer applications	Agencies SHOULD NOT allow personnel to use peer-to-peer applications over the Internet.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	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	
9.3.10.C.01	Receiving files via the Internet	Agencies SHOULD NOT allow personnel to receive files via peer-to-peer, IM or IRC applications.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	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	
9.4.4.C.01	Unescorted access	Agencies MUST ensure that all personnel with unescorted access to TOP SECRET areas have appropriate security clearances and briefings.	Functional	Intersects With	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	5	
9.4.5.C.01	Maintaining an unescorted access list	Agencies MUST maintain an up to date list of personnel entitled to enter a TOP SECRET area without an escort.	Functional	Intersects With	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	5	
9.4.5.C.02	Maintaining an unescorted access list	Personnel MUST display identity cards at all times while within the secure area.	Functional	Intersects With	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	5	
9.4.6.C.01	Displaying the unescorted access list	Agencies SHOULD display within a TOP SECRET area, an up to date list of personnel entitled to enter the area without an escort.	Functional	Intersects With	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	5	
9.4.6.C.02	Displaying the unescorted access list	The unescorted access list SHOULD NOT be visible from outside of the secure area.	Functional	Intersects With	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	5	
9.4.7.C.01	Visitors	Visitors SHOULD be carefully supervised to ensure they do not gain access to or have oversight of information above the level of their clearance or outside of their need-to-know.	Functional	Intersects With	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	5	
9.4.7.C.01	Visitors	Visitors SHOULD be carefully supervised to ensure they do not gain access to or have oversight of information above the level of their clearance or outside of their need-to-know.	Functional	Intersects With	Restrict Unescorted Access	PES-06.3	Physical access control mechanisms exist to restrict unescorted access to facilities to personnel with required security clearances, formal access authorizations and validate the need for access.	5	
9.4.8.C.01	Recording visits in a visitor log	Agencies MUST NOT permit personnel not on the unescorted access list to enter a TOP SECRET area unless their visit is recorded in a visitor log and they are escorted by a person on the unescorted access list.	Functional	Intersects With	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	5	
9.4.9.C.01	Content of the visitor log	Agencies MUST, at minimum, record the following information in a visitor log for each entry: name; organisation; person visiting; contact details for person visiting; and date and time in and out.	Functional	Intersects With	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	5	
9.4.9.C.01	Content of the visitor log	Agencies MUST, at minimum, record the following information in a visitor log for each entry: name; organisation; person visiting; contact details for person visiting; and date and time in and out.	Functional	Intersects With	Automated Records Management & Review	PES-06.4	Automated mechanisms exist to facilitate the maintenance and review of visitor access records.	5	
9.4.9.C.01	Content of the visitor log	Agencies MUST, at minimum, record the following information in a visitor log for each entry: name; organisation; person visiting; contact details for person visiting; and date and time in and out.	Functional	Intersects With	Minimize Visitor Personal Data (PD)	PES-06.5	Mechanisms exist to minimize the collection of Personal Data (PD) contained in visitor access records.	5	
9.4.10.C.01	Separate visitor logs	Agencies with a TOP SECRET area within a larger facility MUST maintain a separate log from any general visitor log.	Functional	Intersects With	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	5	
10.1.42.C.01	Backbone	Agencies MUST use fibre optic cable for backbone infrastructures and installations.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.1.42.C.02	Backbone	Agencies SHOULD use fibre optic cable for backbone infrastructures and installations.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.1.43.C.01	Use of Fibre Optic Cable	Agencies SHOULD use fibre optic cabling.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.1.43.C.02	Use of Fibre Optic Cable	Agencies SHOULD consult with the GCSB where fibre optic cable incorporating conductive metal strengtheners or sheaths is specified.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.1.43.C.03	Use of Fibre Optic Cable	Agencies SHOULD consult with the GCSB where copper cables are specified.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.1.43.C.04	Use of Fibre Optic Cable	Agencies SHOULD NOT use fibre optic cable incorporating conductive metal strengtheners or sheaths except where essential for cable integrity.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.1.44.C.01	Cabling Standards	Agencies MUST install all cabling in accordance with the relevant New Zealand standards as directed by AS/NZS 3000:2007 and NZCSS400.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.1.45.C.01	Cable colours	Agencies MUST comply with the cable and conduit colours specified in the following table. Classification Cable colour Compartmented Information (SCI) Orange/Yellow/Teal or other colour TOP SECRET Red SECRET Blue CONFIDENTIAL Green RESTRICTED and all lower classifications Black	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.1.45.C.02	Cable colours	Additional colours may be used to delineate special networks and compartmented information of the same classification. These networks MUST be labelled and covered in the agency's SOPs.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.1.46.C.01	Cable colours for foreign systems in New Zealand facilities	The cable colour to be used for foreign systems MUST be agreed between the host agency, the foreign system owner and the Accreditation Authority.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.1.46.C.02	Cable colours for foreign systems in New Zealand facilities	Agencies MUST NOT allow cable colours for foreign systems installed in New Zealand facilities to be the same colour as cables used for New Zealand systems.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.1.46.C.03	Cable colours for foreign systems in New Zealand facilities	The cable colour to be used for foreign systems SHOULD be agreed between the host agency, the foreign system owner and the Accreditation Authority.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.1.46.C.04	Cable colours for foreign systems in New Zealand facilities	Agencies SHOULD NOT allow cable colours for foreign systems installed in New Zealand facilities to be the same colour as cables used for New Zealand systems.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.1.47.C.01	Cable groupings	Agencies MUST contact GCSB for advice when combining the cabling of special networks.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	

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
10.1.47.C.02	Cable groupings	Agencies MUST NOT deviate from the approved fibre cable combinations for shared conduits and reticulation systems as indicated below. Group Approved combination 1 UNCLASSIFIED RESTRICTED 2 CONFIDENTIAL SECRET 3 TOP SECRET Other Special Networks	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.1.48.C.01	Fibre optic cables sharing a common conduit	With fibre optic cables the arrangements of fibres within the cable sheath, as illustrated in Figure 3, MUST carry a single classification only.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.1.48.C.02	Fibre optic cables sharing a common conduit	If a fibre optic cable contains subunits, as shown in Figure 4, each subunit MUST carry only a single classification.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.1.48.C.03	Fibre optic cables sharing a common conduit	Agencies MUST NOT mix classifications up to RESTRICTED with classifications of CONFIDENTIAL and above in a single cable.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.1.49.C.01	Audio secure areas	When penetrating an audio secure area for cables, agencies MUST comply with all directions provided by GCSB.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.1.50.C.01	Wall outlet terminations	Cable groups sharing a wall outlet MUST use different connectors for systems of different classifications.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.1.50.C.02	Wall outlet terminations	In areas containing outlets for both TOP SECRET systems and systems of other classifications, agencies MUST ensure that the connectors for the TOP SECRET systems are different to those of the other systems.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.1.50.C.03	Wall outlet terminations	Cable outlets MUST be labelled with the system classification and connector type.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.1.50.C.04	Wall outlet terminations	Cable outlets SHOULD be labelled with the system classification and connector type.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.1.51.C.01	Power Filters	Power filters SHOULD be used to provide a filtered power supply and reduce opportunity for technical attacks.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.2.6.C.01	Cabling Inspection	In TOP SECRET areas or zones, all cabling MUST be inspectable at a minimum of five-metre intervals.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.2.6.C.02	Cabling Inspection	Cabling SHOULD be inspectable at a minimum of five-metre intervals.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.2.7.C.01	Cables sharing a common reticulation system	Approved cable groups may share a common reticulation system but SHOULD have either a dividing partition or a visible gap between the differing cable groups or bundles.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.2.8.C.01	Cabling in walls	Flexible or plastic conduit SHOULD be used in walls to run cabling from cable trays to wall outlets.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.2.9.C.01	Cabinet separation	TOP SECRET cabinets SHOULD have a visible inspectable gap between themselves and lower classified cabinets.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.2.10.C.01	Power Filters	Power filters SHOULD be used to provide a filtered power supply and reduce opportunity for technical attacks.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.3.5.C.01	Use of fibre optic cabling	Agencies SHOULD use fibre optic cabling.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.3.6.C.01	Cabling inspection	In TOP SECRET areas, cables MUST be fully inspectable for their entire length.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.3.6.C.02	Cabling inspection	Cabling SHOULD be inspectable at a minimum of five-metre intervals.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.3.7.C.01	Cables sharing a common reticulation system	Approved cable groups SHOULD have either a dividing partition or a visible gap between the individual cable groups. If the partition or gap exists, cable groups may share a common reticulation system.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.3.8.C.01	Enclosed cable reticulation systems	The front covers of conduits, ducts and cable trays in floors, ceilings and of associated fittings that contain TOP SECRET cabling, SHOULD be clear plastic.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.3.9.C.01	Cabling in walls	Cabling from cable trays to wall outlets SHOULD run in flexible or plastic conduit.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.3.10.C.01	Wall penetrations	For wall penetrations that exit into a lower classified area, cabling SHOULD be encased in conduit with all gaps between the conduit and the wall filled with an appropriate sealing compound.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.3.11.C.01	Power reticulation	TOP SECRET facilities SHOULD have a power distribution board, separately reticulated, located within the TOP SECRET area and supply UPS power to all equipment.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.3.12.C.01	Power Filters	Power filters SHOULD be used to provide a filtered power supply and reduce opportunity for technical attacks.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.3.13.C.01	Cabinet separation	TOP SECRET cabinets SHOULD have a visible gap to separate them from lower classified cabinets.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.4.4.C.01	Use of fibre optic cabling	In TOP SECRET areas, agencies MUST use fibre optic cabling.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.4.4.C.02	Use of fibre optic cabling	Agencies SHOULD use fibre optic cabling.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.4.5.C.01	Cabling inspection	In TOP SECRET areas, cables MUST be fully inspectable for their entire length.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.4.5.C.02	Cabling inspection	Cabling SHOULD be inspectable at a minimum of five-metre intervals.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.4.6.C.01	Cables sharing a common reticulation system	In TOP SECRET areas, approved cable groups can share a common reticulation system but MUST have either a dividing partition or a visible gap between the differing cable groups.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.4.6.C.02	Cables sharing a common reticulation system	TOP SECRET cabling MUST run in a non-shared, enclosed reticulation system.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.4.6.C.03	Cables sharing a common reticulation system	Approved cable groups can share a common reticulation system but SHOULD have either a dividing partition or a visible gap between the differing cable groups.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.4.7.C.01	Enclosed cable reticulation systems	In TOP SECRET areas, the front covers for conduits and cable trays in floors, ceilings and of associated fittings MUST be clear plastic or be inspectable and have tamper proof seals fitted.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.4.7.C.02	Enclosed cable reticulation systems	The front covers of conduits, ducts and cable trays in floors, ceilings and of associated fittings SHOULD be clear plastic or be inspectable and have tamper proof seals fitted.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
10.4.8.C.01	Cabling in walls or party walls	Cabling MUST NOT run in a party wall.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.4.9.C.01	Sealing reticulation systems	Agencies MUST use GCSB endorsed tamper evident seals to seal all removable covers on reticulation systems, including: conduit inspection boxes; outlet and junction boxes; and T-pieces.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.4.9.C.02	Sealing reticulation systems	Tamper evident seals MUST be uniquely identifiable and a register kept of their unique number and location.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.4.9.C.03	Sealing reticulation systems	Conduit joints MUST be sealed with glue or sealant.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.4.9.C.04	Sealing reticulation systems	Conduit joints SHOULD be sealed with glue or sealant.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.4.10.C.01	Wall penetrations	Wall penetrations that exit into a lower classified area, cabling MUST be encased in conduit with all gaps between the conduit and the wall filled with an appropriate sealing compound.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.4.11.C.01	Power reticulation	Secure facilities MUST have a power distribution board located within the secure area and supply UPS power all equipment.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.4.12.C.01	Power Filters	Power filters MUST be used to provide filtered (clean) power and reduce opportunity for technical attacks.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.4.13.C.01	Equipment Cabinet separation	Equipment cabinets MUST have a visible gap or non-conductive isolator between cabinets of different classifications.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.4.13.C.02	Equipment Cabinet separation	There SHOULD be a visible inspectable gap or non-conductive isolator between equipment cabinets of different classifications.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.5.4.C.01	Conduit label specifications	Agencies MUST comply with the conduit label colours specified in the following table. Classification Cable colour Compartmented Information (SCI) Orange/Yellow/Teal or other colour TOP SECRET Red SECRET Blue CONFIDENTIAL Green RESTRICTED and all lower classifications Black	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.5.5.C.01	Installing conduit labelling	Conduit labels installed in public or visitor areas SHOULD NOT be labelled in such a way as to draw attention to or reveal classification of data processed or other agency capability.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.5.6.C.01	Labelling wall outlet boxes	Wall outlet boxes MUST denote the classification, cable and outlet numbers.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.5.6.C.02	Labelling wall outlet boxes	Wall outlet boxes SHOULD denote the classification, cable and outlet numbers.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.5.7.C.01	Standard operating procedures	The SOPs SHOULD record the site conventions for labelling and registration.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.5.8.C.01	Labelling cables	Agencies MUST label cables at each end, with sufficient information to enable the physical identification and inspection of the cable.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.5.8.C.02	Labelling cables	Agencies SHOULD label cables at each end, with sufficient information to enable the physical identification and inspection of the cable.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.5.9.C.01	Cable register	Agencies MUST maintain a register of cables.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.5.9.C.02	Cable register	Agencies SHOULD maintain a register of cables.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.5.10.C.01	Cable register contents	The cable register MUST record at least the following information: cable identification number; classification; socket number, equipment type, source or destination site/floor plan diagram; and seal numbers if applicable.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.5.10.C.02	Cable register contents	The cable register SHOULD record at least the following information: cable identification number; classification; socket number, equipment type, source or destination site/floor plan diagram; and seal numbers if applicable.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.5.11.C.01	Cable inspections	Agencies SHOULD inspect cables for inconsistencies with the cable register in accordance with the frequency defined in the SSP.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.6.22.C.01	Terminations to patch panels	Agencies MUST ensure that only approved cable groups terminate on a patch panel.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.6.22.C.02	Terminations to patch panels	RED and BLACK cables must be separated and bundled.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.6.23.C.01	Patch cable and fly lead connectors	In areas containing cabling for multiple classifications, agencies MUST ensure that the connectors for each classification are distinct and different to those of the other classifications.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.6.23.C.02	Patch cable and fly lead connectors	In areas containing cabling for multiple classifications, agencies MUST document the selection of connector types for each classification.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.6.23.C.03	Patch cable and fly lead connectors	In areas containing cabling for systems of different classifications, agencies SHOULD ensure that the connectors for each system are different to those of the other systems.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.6.23.C.04	Patch cable and fly lead connectors	In areas containing cabling for systems of different classifications, agencies SHOULD document the selection of connector types.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.6.24.C.01	Physical separation of patch panels	Agencies SHOULD physically separate patch panels of different classifications by installing them in separate cabinets.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.6.24.C.02	Physical separation of patch panels	Where spatial constraints demand patch panels of different classification are located in the same cabinet, agencies MUST: provide a physical barrier within the cabinet to separate patch panels; ensure that only personnel cleared to the highest classification of the circuits in the panel have access to the cabinet; and obtain approval from the relevant Accreditation Authority prior to installation.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.6.25.C.01	Cabinet Arrangement	Agencies SHOULD arrange the installation of cabinets as follows: RED equipment at the top; BLACK equipment in the centre; Power equipment at the bottom.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.6.26.C.01	Rack Diagrams	Agencies SHOULD record equipment layouts and other relevant information on rack diagrams.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
10.6.27.C.01	Fly lead installation	Agencies SHOULD ensure that the fibre optic fly leads used to connect wall outlets to IT equipment either: do not exceed 5m in length; or if they exceed 5m in length: are run in the facilitys fixed infrastructure in a protective and easily inspected pathway; are clearly labelled at the equipment end with the wall outlet designator; and are approved by the Accreditation Authority.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.6.28.C.01	Earthing and Bonding	All earthing points MUST be equipotentially bonded.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.6.28.C.02	Earthing and Bonding	All conductive elements of a cabinet, rack or case housing any equipment MUST be earth bonded.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.6.29.C.01	Cable Management	Cabinet rails MUST be installed to: provide adequate room for patch cables and wire managers; provide adequate space for cable management at front, sides, and rear; and arrange switches and patch panels to minimize patching between cabinets & racks.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.6.30.C.01	Labelling Cables	Agencies SHOULD implement the principles and specific cable labelling requirements described above.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.6.31.C.01	Power Cords	Agencies SHOULD follow best practice described above for the installation of power cables.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
10.7.6.C.01	Emanation security threat assessments within New Zealand	Agencies designing and installing systems with RF transmitters within or co-located with their facility MUST: contact GCSB for guidance on conducting an emanation security threat assessment; and install cabling and equipment in accordance with this manual plus any specific installation criteria derived from the emanation security threat assessment.	Functional	Intersects With	Information Leakage Due To Electromagnetic Signals Emanations	PES-13	Facility security mechanisms exist to protect the system from information leakage due to electromagnetic signals emanations.	5	
10.7.6.C.02	Emanation security threat assessments within New Zealand	Agencies designing and installing systems with RF transmitters that co-locate with systems of a classification CONFIDENTIAL and above MUST: contact GCSB for guidance on conducting an emanation security threat assessment; and install cabling and equipment in accordance with this manual plus any specific installation criteria derived from the emanation security threat assessment.	Functional	Intersects With	Information Leakage Due To Electromagnetic Signals Emanations	PES-13	Facility security mechanisms exist to protect the system from information leakage due to electromagnetic signals emanations.	5	
10.7.7.C.01	Emanation security threat assessment outside New Zealand	Agencies deploying systems overseas in temporary, mobile or fixed locations MUST: contact GCSB for assistance with conducting an emanation security threat assessment; and install cabling and equipment in accordance with this manual plus any specific installation criteria derived from the emanation security threat assessment.	Functional	Intersects With	Information Leakage Due To Electromagnetic Signals Emanations	PES-13	Facility security mechanisms exist to protect the system from information leakage due to electromagnetic signals emanations.	5	
10.7.7.C.02	Emanation security threat assessment outside New Zealand	Agencies deploying systems overseas SHOULD: contact GCSB for assistance with conducting an emanation security threat advice; and install cabling and equipment in accordance with this document plus any specific installation criteria derived from the emanation security threat assessment.	Functional	Intersects With	Information Leakage Due To Electromagnetic Signals Emanations	PES-13	Facility security mechanisms exist to protect the system from information leakage due to electromagnetic signals emanations.	5	
10.7.8.C.01	Early identification of emanation security issues	Agencies SHOULD conduct an emanation security threat assessment as early as possible in project lifecycles.	Functional	Intersects With	Information Leakage Due To Electromagnetic Signals Emanations	PES-13	Facility security mechanisms exist to protect the system from information leakage due to electromagnetic signals emanations.	5	
10.7.9.C.01	IT equipment in SECURE areas	Agencies MUST ensure that IT equipment within secure areas meet industry and government standards relating to electromagnetic interference/electromagnetic compatibility.	Functional	Intersects With	Information Leakage Due To Electromagnetic Signals Emanations	PES-13	Facility security mechanisms exist to protect the system from information leakage due to electromagnetic signals emanations.	5	
10.8.34.C.01	Risk Assessment	Agencies MUST conduct and document a risk assessment before creating an architecture, and designing an agency network.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
10.8.34.C.02	Risk Assessment	The principles of separation and segregation as well as the system classification MUST be incorporated into the risk assessment.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
10.8.35.C.01	Security Architecture	Security architectures MUST apply the principles of separation and segregation.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
10.8.36.C.01	Identification of major classifications/categories of network segments	The classification and other restrictions on the security and control of information MUST be clearly identified for each part of the Agency network.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
10.8.37.C.01	Visibility	Systems of different classifications MUST be visually distinct.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
10.8.38.C.01	Information Repository	An information repository, containing essential network information, change records and business requirements SHOULD be established and maintained.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
11.1.15.C.01	Bluetooth within agency environments	Agencies wishing to permit the use of Bluetooth MUST develop a policy that details the circumstances under which Bluetooth usage is permitted, and situations where it is not to be used.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
11.1.15.C.01	Bluetooth within agency environments	Agencies wishing to permit the use of Bluetooth MUST develop a policy that details the circumstances under which Bluetooth usage is permitted, and situations where it is not to be used.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	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.	8	
11.1.15.C.02	Bluetooth within agency environments	The policy position MUST include information about Bluetooth security controls that are to be used, and methods for verifying that the controls are in place and are effective.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
11.1.16.C.01	Bluetooth connections	Agencies MUST ensure that Bluetooth pairing is only established between authorised devices. (Unless a gateway is being used, paired devices are considered to operate at the same security classification level).	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
11.1.16.C.02	Bluetooth connections	Agencies SHOULD ensure that Bluetooth discovery of devices is disabled unless a new pairing connection is being established.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
11.1.16.C.03	Bluetooth connections	Agencies SHOULD ensure that Bluetooth device pairing only occurs at a location where only authorised persons have access.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	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	
11.1.16.C.04	Bluetooth connections	Agencies SHOULD ensure that Bluetooth pairings are removed when they are no longer required.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	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	
11.1.17.C.01	Bluetooth versions	Agencies using Bluetooth MUST use the most secure configuration supported by the paired devices.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
11.1.17.C.02	Bluetooth versions	Agencies SHOULD identify the: Bluetooth type (BR/EDR or LE), version, and security capabilities; for devices used to form Bluetooth connections, and ensure they are used to inform risk decisions on the use of Bluetooth.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	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	
11.1.17.C.03	Bluetooth versions	Agencies SHOULD ensure that new Bluetooth connections between devices are authenticated using explicit user actions, such as entry of a numeric code, confirmation of a matching PIN, or other affirming action, such as challenge-response process.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
11.1.18.C.01	Encryption and authentication protocols	Agencies using Bluetooth between devices to transfer UNCLASSIFIED or IN-CONFIDENCE information SHOULD ensure that connections meet NZISM standards for authentication and use Approved Cryptographic Algorithms for encryption and message integrity.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	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	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
11.1.18.C.02	Encryption and authentication protocols	Agencies using Bluetooth between devices to transfer RESTRICTED or SENSITIVE information MUST ensure that connections meet NZISM standards for authentication and use Approved Cryptographic Algorithms for encryption and message integrity.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	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	
11.1.18.C.03	Encryption and authentication protocols	If Bluetooth specifications do not support these approved encryption methods, organisations MUST do a risk assessment and use the exception or waiver process to accept this risk.	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
11.1.19.C.01	Bluetooth in secure areas	Agencies MUST complete a technical evaluation of the secure area, consult the relevant technical authority and seek approval from the Accreditation Authority before permitting the use of Bluetooth devices.	Functional	Intersects With	Assessments	IAO-02	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.	8	
11.1.19.C.02	Bluetooth in secure areas	Agencies using Bluetooth devices MUST NOT allow: line of sight and reflected communications travelling into an unsecure area. multiple Bluetooth devices at different classifications in the same area.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	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	
11.1.19.C.03	Bluetooth in secure areas	Agencies MUST NOT allow Bluetooth devices into secure areas unless authorised by the Accreditation Authority.	Functional	Intersects With	Bluetooth & Wireless Devices	AST-14.1	Mechanisms exist to prevent the usage of Bluetooth and wireless devices (e.g., Near Field Communications (NFC)) in sensitive areas or unless used in a Radio Frequency (RF)-screened building.	5	
11.2.11.C.01	RF devices in secure areas	Agencies MUST prevent RF devices from being brought into secure areas unless authorised by the Accreditation Authority.	Functional	Intersects With	Multi-Function Devices (MFD)	AST-23	Mechanisms exist to securely configure Multi-Function Devices (MFD) according to industry-recognized secure practices for the type of device.	5	
11.2.11.C.02	RF devices in secure areas	Agencies SHOULD prevent RF devices from being brought into secure areas unless authorised by the Accreditation Authority.	Functional	Intersects With	Multi-Function Devices (MFD)	AST-23	Mechanisms exist to securely configure Multi-Function Devices (MFD) according to industry-recognized secure practices for the type of device.	5	
11.2.12.C.01	RF controls in secure areas	Agencies SHOULD limit the effective range of communications outside the agency's area of control by: minimising the output power level of wireless devices; RF shielding; and Physical layout and separation.	Functional	Intersects With	Multi-Function Devices (MFD)	AST-23	Mechanisms exist to securely configure Multi-Function Devices (MFD) according to industry-recognized secure practices for the type of device.	5	
11.2.13.C.01	Detecting RF devices in secure areas	Agencies SHOULD deploy measures to detect and respond to active RF devices within secure areas.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
11.2.13.C.01	Detecting RF devices in secure areas	Agencies SHOULD deploy measures to detect and respond to active RF devices within secure areas.	Functional	Intersects With	Multi-Function Devices (MFD)	AST-23	Mechanisms exist to securely configure Multi-Function Devices (MFD) according to industry-recognized secure practices for the type of device.	5	
11.2.14.C.01	Pointing devices	Wireless RF or IR pointing devices MUST NOT be used in secure areas unless approved by the Accreditation Authority and appropriate RF or IR mitigations are implemented.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	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	
11.2.15.C.01	IR devices in secure areas	Agencies using infrared keyboards MUST NOT allow: line of sight and reflected communications travelling into an unsecure area; multiple infrared keyboards at different classifications in the same area; other infrared devices to be brought into line of sight of the keyboard or its receiving device/port; and infrared keyboards to be operated in areas with unprotected windows.	Functional	Intersects With	Infrared Communications	AST-14.2	Mechanisms exist to prevent line of sight and reflected infrared (IR) communications use in an unsecured space.	5	
11.2.15.C.01	IR devices in secure areas	Agencies using infrared keyboards MUST NOT allow: line of sight and reflected communications travelling into an unsecure area; multiple infrared keyboards at different classifications in the same area; other infrared devices to be brought into line of sight of the keyboard or its receiving device/port; and infrared keyboards to be operated in areas with unprotected windows.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	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	
11.2.15.C.02	IR devices in secure areas	Agencies using infrared keyboards MUST NOT allow: line of sight and reflected communications travelling into an unsecure area; multiple infrared keyboards at different classifications in the same area; other infrared devices within the same area; and infrared keyboards in areas with windows that have not had a permanent method of blocking infrared transmissions applied to them.	Functional	Intersects With	Infrared Communications	AST-14.2	Mechanisms exist to prevent line of sight and reflected infrared (IR) communications use in an unsecured space.	5	
11.2.15.C.02	IR devices in secure areas	Agencies using infrared keyboards MUST NOT allow: line of sight and reflected communications travelling into an unsecure area; multiple infrared keyboards at different classifications in the same area; other infrared devices within the same area; and infrared keyboards in areas with windows that have not had a permanent method of blocking infrared transmissions applied to them.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	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	
11.2.15.C.03	IR devices in secure areas	Agencies using IR devices SHOULD ensure that the IR receiver/port is positioned to prevent line of sight from the secure area boundary.	Functional	Intersects With	Infrared Communications	AST-14.2	Mechanisms exist to prevent line of sight and reflected infrared (IR) communications use in an unsecured space.	5	
11.2.15.C.03	IR devices in secure areas	Agencies using IR devices SHOULD ensure that the IR receiver/port is positioned to prevent line of sight from the secure area boundary.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	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	
11.3.5.C.01	Telephones and telephone systems usage policy	Agencies MUST develop a policy governing the use of telephones and telephone systems.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
11.3.5.C.01	Telephones and telephone systems usage policy	Agencies MUST develop a policy governing the use of telephones and telephone systems.	Functional	Intersects With	Telecommunications Equipment	AST-19	Mechanisms exist to establish usage restrictions and implementation guidance for telecommunication equipment to prevent potential damage or unauthorized modification and to prevent potential eavesdropping.	5	
11.3.6.C.01	Personnel awareness	Agencies MUST advise personnel of the maximum permitted classification for conversations using both internal and external telephone connections.	Functional	Intersects With	Telecommunications Equipment	AST-19	Mechanisms exist to establish usage restrictions and implementation guidance for telecommunication equipment to prevent potential damage or unauthorized modification and to prevent potential eavesdropping.	5	
11.3.6.C.02	Personnel awareness	Agencies SHOULD advise personnel of the audio security risk posed by using telephones in areas where classified conversations can occur.	Functional	Intersects With	Telecommunications Equipment	AST-19	Mechanisms exist to establish usage restrictions and implementation guidance for telecommunication equipment to prevent potential damage or unauthorized modification and to prevent potential eavesdropping.	5	
11.3.7.C.01	Visual indication	Agencies permitting different levels of conversation for different types of connections MUST use telephones that give a visual indication of the classification of the connection made.	Functional	Intersects With	Telecommunications Equipment	AST-19	Mechanisms exist to establish usage restrictions and implementation guidance for telecommunication equipment to prevent potential damage or unauthorized modification and to prevent potential eavesdropping.	5	
11.3.8.C.01	Use of telephone systems	Agencies intending to use telephone systems for the transmission of classified information MUST ensure that: the system has been accredited for the purpose; and all classified traffic that passes over external systems is appropriately encrypted.	Functional	Intersects With	Telecommunications Equipment	AST-19	Mechanisms exist to establish usage restrictions and implementation guidance for telecommunication equipment to prevent potential damage or unauthorized modification and to prevent potential eavesdropping.	5	
11.3.9.C.01	Cordless telephones	Agencies MUST NOT use cordless telephones for classified conversations.	Functional	Intersects With	Telecommunications Equipment	AST-19	Mechanisms exist to establish usage restrictions and implementation guidance for telecommunication equipment to prevent potential damage or unauthorized modification and to prevent potential eavesdropping.	5	
11.3.9.C.02	Cordless telephones	Agencies SHOULD NOT use cordless telephones for classified or sensitive conversations.	Functional	Intersects With	Telecommunications Equipment	AST-19	Mechanisms exist to establish usage restrictions and implementation guidance for telecommunication equipment to prevent potential damage or unauthorized modification and to prevent potential eavesdropping.	5	
11.3.10.C.01	Cordless telephones with secure telephony devices	Agencies MUST NOT use cordless telephones in conjunction with secure telephony devices.	Functional	Intersects With	Telecommunications Equipment	AST-19	Mechanisms exist to establish usage restrictions and implementation guidance for telecommunication equipment to prevent potential damage or unauthorized modification and to prevent potential eavesdropping.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
11.3.11.C.01	Speakerphones	If a speakerphone is to be used on a secure telephone system within a secure area, agencies MUST apply the following controls: it is located in a room rated as audio secure; the room is audio secure during any conversations; only cleared personnel involved in discussions are present in the room; and ensure approval for this exception is granted by the Accreditation Authority.	Functional	Intersects With	Telecommunications Equipment	AST-19	Mechanisms exist to establish usage restrictions and implementation guidance for telecommunication equipment to prevent potential damage or unauthorized modification and to prevent potential eavesdropping.	5	
11.3.12.C.01	Off-hook audio protection	Agencies MUST ensure that off-hook audio protection features are used on all telephones that are not accredited for the transmission of classified information in areas where such information could be discussed.	Functional	Intersects With	Telecommunications Equipment	AST-19	Mechanisms exist to establish usage restrictions and implementation guidance for telecommunication equipment to prevent potential damage or unauthorized modification and to prevent potential eavesdropping.	5	
11.3.12.C.02	Off-hook audio protection	Agencies MUST use push-to-talk mechanisms to meet the requirement for off-hook audio protection. PTT activation MUST be clearly labelled.	Functional	Intersects With	Telecommunications Equipment	AST-19	Mechanisms exist to establish usage restrictions and implementation guidance for telecommunication equipment to prevent potential damage or unauthorized modification and to prevent potential eavesdropping.	5	
11.3.12.C.03	Off-hook audio protection	Agencies SHOULD ensure that off-hook audio protection features are used on all telephones that are not accredited for the transmission of classified information in areas where such information could be discussed.	Functional	Intersects With	Telecommunications Equipment	AST-19	Mechanisms exist to establish usage restrictions and implementation guidance for telecommunication equipment to prevent potential damage or unauthorized modification and to prevent potential eavesdropping.	5	
11.3.13.C.01	Electronic Records Retention and Voicemail	Agencies MUST remove unused voice mailboxes.	Functional	Intersects With	Telecommunications Equipment	AST-19	Mechanisms exist to establish usage restrictions and implementation guidance for telecommunication equipment to prevent potential damage or unauthorized modification and to prevent potential eavesdropping.	5	
11.3.13.C.01	Electronic Records Retention and Voicemail	Agencies MUST remove unused voice mailboxes.	Functional	Intersects With	Electronic Discovery (eDiscovery)	BCD-12.3	Mechanisms exist to utilize electronic discovery (eDiscovery) that covers current and archived communication transactions.	5	
11.3.13.C.02	Electronic Records Retention and Voicemail	Agencies MUST expire and archive or delete voicemail messages after the retention period determined by the agency's electronic records retention policy.	Functional	Intersects With	Telecommunications Equipment	AST-19	Mechanisms exist to establish usage restrictions and implementation guidance for telecommunication equipment to prevent potential damage or unauthorized modification and to prevent potential eavesdropping.	5	
11.3.13.C.02	Electronic Records Retention and Voicemail	Agencies MUST expire and archive or delete voicemail messages after the retention period determined by the agency's electronic records retention policy.	Functional	Intersects With	Electronic Discovery (eDiscovery)	BCD-12.3	Mechanisms exist to utilize electronic discovery (eDiscovery) that covers current and archived communication transactions.	5	
11.3.13.C.03	Electronic Records Retention and Voicemail	Agencies SHOULD develop and implement a policy to manage the retention and disposal of such electronic records, including voicemail, email and other electronic records.	Functional	Intersects With	Telecommunications Equipment	AST-19	Mechanisms exist to establish usage restrictions and implementation guidance for telecommunication equipment to prevent potential damage or unauthorized modification and to prevent potential eavesdropping.	5	
11.3.13.C.03	Electronic Records Retention and Voicemail	Agencies SHOULD develop and implement a policy to manage the retention and disposal of such electronic records, including voicemail, email and other electronic records.	Functional	Intersects With	Electronic Discovery (eDiscovery)	BCD-12.3	Mechanisms exist to utilize electronic discovery (eDiscovery) that covers current and archived communication transactions.	5	
11.4.9.C.01	Mobile device usage policy	Agencies MUST develop a policy governing the use of mobile devices.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
11.4.9.C.01	Mobile device usage policy	Agencies MUST develop a policy governing the use of mobile devices.	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
11.4.10.C.01	Personnel awareness	Agencies MUST advise personnel of the maximum permitted classification for conversations using both internal and external mobile devices.	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
11.4.10.C.02	Personnel awareness	Agencies SHOULD advise personnel of all known security risks posed by using mobile devices in areas where classified conversations can occur.	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
11.4.11.C.01	Use of mobile devices	Agencies intending to use mobile devices for the transmission of classified information MUST ensure that: the network has been certified and accredited for the purpose; all classified traffic that passes over mobile devices is appropriately encrypted; and users are aware of the area, surroundings, potential for overhearing and potential for oversight when using the device.	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
11.4.12.C.01	Mobile Device Physical Security	Mobile devices MUST be prevented from entering secure areas.	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
11.4.12.C.02	Mobile Device Physical Security	Agencies SHOULD provide a storage area or lockers where mobile devices can be stored before personnel enter secure or protected areas.	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
11.5.13.C.01	Personal Wearable Device usage policy	Agencies MUST develop a policy governing the use of personal wearable devices, including fitness devices.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
11.5.13.C.01	Personal Wearable Device usage policy	Agencies MUST develop a policy governing the use of personal wearable devices, including fitness devices.	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
11.5.14.C.01	Personnel awareness	Agencies MUST advise personnel of the maximum permitted classification for conversations where any personal wearable or mobile device may be present.	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
11.5.14.C.02	Personnel awareness	Agencies SHOULD advise personnel of all known security risks posed by using personal wearable devices in secure areas or other areas where classified conversations can occur.	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
11.5.15.C.01	Mobile Device Physical Security	Personal wearable devices MUST NOT be allowed to enter secure areas.	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
11.5.15.C.02	Mobile Device Physical Security	Agencies SHOULD provide a storage area or lockers where personal wearable devices can be stored before personnel enter secure or protected areas.	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
11.5.16.C.01	Medical Exemptions	Any personal wearable devices approved on medical grounds MUST NOT have any of the following capabilities: Camera; Microphone; Voice/video/still photograph recording; Cellular, Wi-Fi or other RF means of transmission.	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
11.5.16.C.02	Medical Exemptions	Where personal wearable devices are exempted on medical grounds and used in secure areas agencies MUST ensure that: the agency networks in secure areas have been certified and accredited for the purpose; and users are aware of the area, surroundings, potential for overhearing and potential for oversight.	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
11.5.16.C.03	Medical Exemptions	Where the use of personal wearable devices is permitted on medical grounds and used within a corporate or agency environment, agencies MUST ensure any relevant legislation and regulation pertaining to the protection of personal information is followed.	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
11.6.59.C.01	Risk Assessment	Agencies MUST conduct and document a risk assessment before implementing or adopting an RFID solution.	Functional	Intersects With	Radio Frequency Identification (RFID) Security	AST-29	Mechanisms exist to securely govern Radio Frequency Identification (RFID) deployments to ensure RFID is used safely and securely to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.6.59.C.02	Risk Assessment	This risk assessment MUST be the basis of a security architecture design.	Functional	Intersects With	Radio Frequency Identification (RFID) Security	AST-29	Mechanisms exist to securely govern Radio Frequency Identification (RFID) deployments to ensure RFID is used safely and securely to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.6.60.C.01	Security Architecture	Agencies MUST develop a strong security architecture to protect RFID databases and RFID systems.	Functional	Intersects With	Radio Frequency Identification (RFID) Security	AST-29	Mechanisms exist to securely govern Radio Frequency Identification (RFID) deployments to ensure RFID is used safely and securely to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.6.60.C.02	Security Architecture	Agencies MUST minimise the information stored on RFID tags and in the RFID subsystem.	Functional	Intersects With	Radio Frequency Identification (RFID) Security	AST-29	Mechanisms exist to securely govern Radio Frequency Identification (RFID) deployments to ensure RFID is used safely and securely to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.6.60.C.03	Security Architecture	Agencies SHOULD disable any rewrite functions on RFID devices.	Functional	Intersects With	Radio Frequency Identification (RFID) Security	AST-29	Mechanisms exist to securely govern Radio Frequency Identification (RFID) deployments to ensure RFID is used safely and securely to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.6.60.C.04	Security Architecture	Agencies SHOULD apply the access control requirements of the NZISM (Chapter 11 - Communications Systems and Devices) to RFID systems.	Functional	Intersects With	Radio Frequency Identification (RFID) Security	AST-29	Mechanisms exist to securely govern Radio Frequency Identification (RFID) deployments to ensure RFID is used safely and securely to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	

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
11.6.61.C.01	Policy	Agencies SHOULD develop, implement and maintain an RFID Usage Policy.	Functional	Intersects With	Radio Frequency Identification (RFID) Security	AST-29	Mechanisms exist to securely govern Radio Frequency Identification (RFID) deployments to ensure RFID is used safely and securely to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.6.61.C.02	Policy	Agencies SHOULD incorporate RFID into the agency's security policies and information security documentation.	Functional	Intersects With	Radio Frequency Identification (RFID) Security	AST-29	Mechanisms exist to securely govern Radio Frequency Identification (RFID) deployments to ensure RFID is used safely and securely to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.6.62.C.01	Inspections	Agencies MUST conduct visual and technical inspections of packaging and devices to determine if RFID devices have been attached and either permanently disable or remove such devices.	Functional	Intersects With	Radio Frequency Identification (RFID) Security	AST-29	Mechanisms exist to securely govern Radio Frequency Identification (RFID) deployments to ensure RFID is used safely and securely to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.6.62.C.02	Inspections	Agencies SHOULD conduct visual inspections of packaging and devices to determine if RFID devices have been attached and if these RFID devices pose a security concern.	Functional	Intersects With	Radio Frequency Identification (RFID) Security	AST-29	Mechanisms exist to securely govern Radio Frequency Identification (RFID) deployments to ensure RFID is used safely and securely to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.6.62.C.03	Inspections	Agencies SHOULD conduct visual inspections of packaging and devices to determine if RFID devices or labelling have been tampered with and whether this is a security concern.	Functional	Intersects With	Radio Frequency Identification (RFID) Security	AST-29	Mechanisms exist to securely govern Radio Frequency Identification (RFID) deployments to ensure RFID is used safely and securely to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.6.63.C.01	Shielding	Agencies SHOULD consider undertaking an RF engineering assessment where security concerns exist or where the RFID systems are to be used in areas with high levels of RF activity.	Functional	Intersects With	Radio Frequency Identification (RFID) Security	AST-29	Mechanisms exist to securely govern Radio Frequency Identification (RFID) deployments to ensure RFID is used safely and securely to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.6.63.C.02	Shielding	Shielding SHOULD be considered where eavesdropping or RF radiation is a concern, as determined by the risk assessment.	Functional	Intersects With	Radio Frequency Identification (RFID) Security	AST-29	Mechanisms exist to securely govern Radio Frequency Identification (RFID) deployments to ensure RFID is used safely and securely to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.6.64.C.01	Positioning of Tags and Readers	Agencies SHOULD consider placement of tags and location of readers to avoid unnecessary electromagnetic radiation.	Functional	Intersects With	Radio Frequency Identification (RFID) Security	AST-29	Mechanisms exist to securely govern Radio Frequency Identification (RFID) deployments to ensure RFID is used safely and securely to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.6.65.C.01	Encoding and Encryption	Agencies MUST follow the requirements of the NZISM in the selection and implementation of cryptographic protocols and algorithms, and in key management, detailed in Chapter 17 - Cryptography.	Functional	Intersects With	Radio Frequency Identification (RFID) Security	AST-29	Mechanisms exist to securely govern Radio Frequency Identification (RFID) deployments to ensure RFID is used safely and securely to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.6.65.C.02	Encoding and Encryption	Agencies SHOULD encrypt data before it is written to RFID tags.	Functional	Intersects With	Radio Frequency Identification (RFID) Security	AST-29	Mechanisms exist to securely govern Radio Frequency Identification (RFID) deployments to ensure RFID is used safely and securely to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.6.65.C.03	Encoding and Encryption	Agencies SHOULD assign RFID identifiers using formats that limit information about tagged items or about the agency operating the RFID system.	Functional	Intersects With	Radio Frequency Identification (RFID) Security	AST-29	Mechanisms exist to securely govern Radio Frequency Identification (RFID) deployments to ensure RFID is used safely and securely to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.6.66.C.01	Authentication	Agencies SHOULD consider the use of HMAC when tag authenticity is required.	Functional	Intersects With	Radio Frequency Identification (RFID) Security	AST-29	Mechanisms exist to securely govern Radio Frequency Identification (RFID) deployments to ensure RFID is used safely and securely to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.6.67.C.01	Password Management	Agencies MUST assign passwords for critical RFID functions.	Functional	Intersects With	Radio Frequency Identification (RFID) Security	AST-29	Mechanisms exist to securely govern Radio Frequency Identification (RFID) deployments to ensure RFID is used safely and securely to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.6.67.C.02	Password Management	Agencies SHOULD follow the guidance for passwords management in the NZISM (Chapter 16 - Access control and passwords).	Functional	Intersects With	Radio Frequency Identification (RFID) Security	AST-29	Mechanisms exist to securely govern Radio Frequency Identification (RFID) deployments to ensure RFID is used safely and securely to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.6.68.C.01	Temporary Deactivation of Tags	Agencies SHOULD consider temporary deactivation of RFID tags where the tag is likely to be inactive for extended periods.	Functional	Intersects With	Radio Frequency Identification (RFID) Security	AST-29	Mechanisms exist to securely govern Radio Frequency Identification (RFID) deployments to ensure RFID is used safely and securely to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.6.69.C.01	Incident Management	Agencies MUST develop and implement incident identification and management processes in accordance with this manual (See Chapter 5 - Information Security Documentation, Chapter 6 - Information Security Monitoring, Chapter 7 - Information Security Incidents, Chapter 9 - Personnel Security and Chapter 16 - Access Control and passwords).	Functional	Intersects With	Radio Frequency Identification (RFID) Security	AST-29	Mechanisms exist to securely govern Radio Frequency Identification (RFID) deployments to ensure RFID is used safely and securely to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.6.70.C.01	Disposal	Agencies SHOULD consider secure disposal procedures and incorporate these into the RFID Usage Policy. Refer also to Chapter 13 - Media and IT equipment management, decommissioning and disposal.	Functional	Intersects With	Radio Frequency Identification (RFID) Security	AST-29	Mechanisms exist to securely govern Radio Frequency Identification (RFID) deployments to ensure RFID is used safely and securely to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.6.71.C.01	Operator Training and User Awareness	Agencies MUST develop and implement user awareness and training programmes to support and enable safe use of RFID services (See Section 9.1 - Information Security Awareness and Training).	Functional	Intersects With	Radio Frequency Identification (RFID) Security	AST-29	Mechanisms exist to securely govern Radio Frequency Identification (RFID) deployments to ensure RFID is used safely and securely to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.7.29.C.01	Risk Assessment	Agencies MUST conduct and document a risk assessment before implementing or adopting an RFID access card system.	Functional	Intersects With	Contactless Access Control Systems	AST-29.1	Mechanisms exist to securely configure contactless access control systems incorporating contactless RFID or smart cards to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.7.29.C.02	Risk Assessment	This risk assessment MUST be the basis of a security architecture design.	Functional	Intersects With	Contactless Access Control Systems	AST-29.1	Mechanisms exist to securely configure contactless access control systems incorporating contactless RFID or smart cards to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.7.30.C.01	Security Architecture	Agencies MUST develop a strong security architecture to protect access to databases and systems.	Functional	Intersects With	Contactless Access Control Systems	AST-29.1	Mechanisms exist to securely configure contactless access control systems incorporating contactless RFID or smart cards to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.7.30.C.02	Security Architecture	Agencies SHOULD apply the NZISM access controls (Chapter 11) and cryptographic controls (Chapter 17) to access card systems.	Functional	Intersects With	Contactless Access Control Systems	AST-29.1	Mechanisms exist to securely configure contactless access control systems incorporating contactless RFID or smart cards to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.7.30.C.03	Security Architecture	Agencies SHOULD consider the application of the following design elements: Implement a Demilitarized Zone (DMZ) to isolate card systems from other parts of the organisations network and from high-risk Internet Protocol (IP) network connections; Secure or remove connections between the Internet and card system network segments; Secure or remove vulnerable dialup modem links; Secure or remove vulnerable wireless radio links and network access points; and Network activity monitoring for unusual or anomalous access activity and well as intrusion detection.	Functional	Intersects With	Contactless Access Control Systems	AST-29.1	Mechanisms exist to securely configure contactless access control systems incorporating contactless RFID or smart cards to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.7.31.C.01	Policy	Agencies SHOULD develop, implement and maintain an Access Card Usage Policy.	Functional	Intersects With	Contactless Access Control Systems	AST-29.1	Mechanisms exist to securely configure contactless access control systems incorporating contactless RFID or smart cards to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.7.31.C.02	Policy	Agencies SHOULD incorporate access cards into the agency's security policies and information security documentation.	Functional	Intersects With	Contactless Access Control Systems	AST-29.1	Mechanisms exist to securely configure contactless access control systems incorporating contactless RFID or smart cards to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.7.32.C.01	Physical Security	Agencies SHOULD select systems that provide resistance to physical or electronic tampering.	Functional	Intersects With	Contactless Access Control Systems	AST-29.1	Mechanisms exist to securely configure contactless access control systems incorporating contactless RFID or smart cards to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.7.32.C.02	Physical Security	Agencies SHOULD implement systems to minimise the risk of physical or electronic tampering.	Functional	Intersects With	Contactless Access Control Systems	AST-29.1	Mechanisms exist to securely configure contactless access control systems incorporating contactless RFID or smart cards to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
11.7.32.C.03	Physical Security	Agencies SHOULD consider placement of tags and location of readers to avoid unnecessary electromagnetic radiation.	Functional	Intersects With	Contactless Access Control Systems	AST-29.1	Mechanisms exist to securely configure contactless access control systems incorporating contactless RFID or smart cards to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.7.32.C.04	Physical Security	Agencies SHOULD consider and select other physical controls in accordance with the PSR.	Functional	Intersects With	Contactless Access Control Systems	AST-29.1	Mechanisms exist to securely configure contactless access control systems incorporating contactless RFID or smart cards to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.7.33.C.01	Card Data Protection	Agencies MUST follow the requirements of the NZISM in the selection and implementation of cryptographic protocols and algorithms, and in key management, detailed in Chapter 17 - Cryptography.	Functional	Intersects With	Contactless Access Control Systems	AST-29.1	Mechanisms exist to securely configure contactless access control systems incorporating contactless RFID or smart cards to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.7.33.C.02	Card Data Protection	Agencies SHOULD encrypt data before it is written to cards.	Functional	Intersects With	Contactless Access Control Systems	AST-29.1	Mechanisms exist to securely configure contactless access control systems incorporating contactless RFID or smart cards to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.7.33.C.03	Card Data Protection	Agencies SHOULD consider the use of cards systems incorporating Secure Access Modules (SAMs).	Functional	Intersects With	Contactless Access Control Systems	AST-29.1	Mechanisms exist to securely configure contactless access control systems incorporating contactless RFID or smart cards to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.7.34.C.01	Incident Management	Agencies MUST develop and implement incident identification and management processes in accordance with this manual (See Chapter 5 - Information Security Documentation, Chapter 6 - Information Security Monitoring, Chapter 7 - Information Security Incidents, Chapter 9 - Personnel Security and Chapter 16 - Access control and passwords).	Functional	Intersects With	Contactless Access Control Systems	AST-29.1	Mechanisms exist to securely configure contactless access control systems incorporating contactless RFID or smart cards to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.	5	
11.7.35.C.01	Disposal	Agencies SHOULD consider secure disposal procedures and incorporate these into the Access Card Usage Policy. Refer also to Media and IT equipment management, decommissioning and disposal.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
11.7.35.C.01	Disposal	Agencies SHOULD consider secure disposal procedures and incorporate these into the Access Card Usage Policy. Refer also to Media and IT equipment management, decommissioning and disposal.	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
11.8.3.C.01	MFD, network printer and fax machine usage policy	Agencies MUST develop a policy governing the use of MFDs, network printers and fax machines,	Functional	Intersects With	Telecommunications Equipment	AST-19	Mechanisms exist to establish usage restrictions and implementation guidance for telecommunication equipment to prevent potential damage or unauthorized modification and to prevent potential eavesdropping.	5	
11.8.3.C.01	MFD, network printer and fax machine usage policy	Agencies MUST develop a policy governing the use of MFDs, network printers and fax machines,	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
11.8.3.C.01	MFD, network printer and fax machine usage policy	Agencies MUST develop a policy governing the use of MFDs, network printers and fax machines,	Functional	Intersects With	Multi-Function Devices (MFD)	AST-23	Mechanisms exist to securely configure Multi-Function Devices (MFD) according to industry-recognized secure practices for the type of device.	8	
11.8.4.C.01	Sending fax messages	Agencies sending classified messages MUST ensure that the message is encrypted to an appropriate level when communicated over unsecured telecommunications infrastructure or the public switched telephone network.	Functional	Intersects With	Telecommunications Equipment	AST-19	Mechanisms exist to establish usage restrictions and implementation guidance for telecommunication equipment to prevent potential damage or unauthorized modification and to prevent potential eavesdropping.	5	
11.8.4.C.01	Sending fax messages	Agencies sending classified messages MUST ensure that the message is encrypted to an appropriate level when communicated over unsecured telecommunications infrastructure or the public switched telephone network.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	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	
11.8.4.C.02	Sending fax messages	Agencies MUST have separate MFDs or fax machines for sending classified messages and messages classified RESTRICTED and below.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	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	
11.8.5.C.01	Receiving fax messages	The sender of a fax message SHOULD make arrangements for the receiver to: collect the fax message as soon as possible after it is received; and notify the sender immediately if the fax message does not arrive when expected.	Functional	Intersects With	Telecommunications Equipment	AST-19	Mechanisms exist to establish usage restrictions and implementation guidance for telecommunication equipment to prevent potential damage or unauthorized modification and to prevent potential eavesdropping.	5	
11.8.5.C.01	Receiving fax messages	The sender of a fax message SHOULD make arrangements for the receiver to: collect the fax message as soon as possible after it is received; and notify the sender immediately if the fax message does not arrive when expected.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	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	
11.8.6.C.01	Connecting MFDs to telephone networks	Agencies MUST NOT enable a direct connection from a MFD to a telephone network unless the telephone network is accredited to at least the same classification as the computer network to which the device is connected.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
11.8.6.C.01	Connecting MFDs to telephone networks	Agencies MUST NOT enable a direct connection from a MFD to a telephone network unless the telephone network is accredited to at least the same classification as the computer network to which the device is connected.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	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	
11.8.6.C.02	Connecting MFDs to telephone networks	Agencies SHOULD NOT enable a direct connection from a MFD to a telephone network unless the telephone network is accredited to at least the same classification as the computer network to which the device is connected.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
11.8.6.C.02	Connecting MFDs to telephone networks	Agencies SHOULD NOT enable a direct connection from a MFD to a telephone network unless the telephone network is accredited to at least the same classification as the computer network to which the device is connected.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	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	
11.8.7.C.01	Connecting MFDs to computer networks	Where MFDs connected to computer networks have the ability to communicate via a gateway to another network, agencies MUST ensure that: each MFD applies user identification, authentication and audit functions for all classified information communicated by that device; these mechanisms are of similar strength to those specified for workstations on that network; and each gateway can identify and filter the classified information in accordance with the requirements for the export of data through a gateway.	Functional	Intersects With	Multi-Function Devices (MFD)	AST-23	Mechanisms exist to securely configure Multi-Function Devices (MFD) according to industry-recognized secure practices for the type of device.	5	
11.8.8.C.01	Copying documents on MFDs	Agencies MUST NOT permit MFDs connected to computer networks to be used to scan or copy classified documents above the classification of the connected network.	Functional	Intersects With	Multi-Function Devices (MFD)	AST-23	Mechanisms exist to securely configure Multi-Function Devices (MFD) according to industry-recognized secure practices for the type of device.	5	
11.8.9.C.01	Observing MFD and fax machine use	Agencies SHOULD ensure that MFDs and fax machines are located in areas where their use can be observed.	Functional	Intersects With	Access Control for Output Devices	PES-12.2	Physical security mechanisms exist to restrict access to printers and other system output devices to prevent unauthorized individuals from obtaining the output.	5	
11.8.10.C.01	Servicing and Maintenance	Any maintenance or servicing MUST be conducted under supervision or by cleared personnel.	Functional	Intersects With	Controlled Maintenance	MNT-02	Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application and/or Service (TAAS).	5	
11.8.10.C.02	Servicing and Maintenance	Any storage devices, drums or cartridges with memory chips removed during maintenance or servicing MUST be disposed of following the processes prescribed in Chapter 13 - Media and IT equipment Management, Decommissioning and Disposal.	Functional	Intersects With	Prevent Unauthorized Removal	MNT-04.3	Mechanisms exist to prevent or control the removal of equipment undergoing maintenance that contains organizational information.	5	
11.8.10.C.03	Servicing and Maintenance	Toner cartridges MUST have the memory chip removed before the cartridge is recycled or otherwise disposed of. The memory chip MUST be disposed of following the processes prescribed in Chapter 13 - Media and IT equipment Management, Decommissioning and Disposal.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
11.8.10.C.04	Servicing and Maintenance	Any maintenance or servicing SHOULD be conducted under supervision or by cleared personnel.	Functional	Intersects With	Controlled Maintenance	MNT-02	Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application and/or Service (TAAS).	5	
11.8.10.C.05	Servicing and Maintenance	Any storage devices, drums or cartridges with memory chips removed during maintenance or servicing SHOULD be disposed of following the processes prescribed in Chapter 13 - Media and IT equipment Management, Decommissioning and Disposal.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
11.8.11.C.01	USB Devices	The use of any USB capability MUST be conducted under supervision or by cleared personnel.	Functional	Intersects With	Portable Storage Devices	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.	5	
11.8.11.C-02	USB Devices	The use of any USB capability SHOULD be conducted under supervision or by cleared personnel.	Functional	Intersects With	Portable Storage Devices	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
11.8.12.C.01	Decommissioning and Disposal	Any storage devices, drums, cartridge memory chips or other components that may contain data or copies of documents MUST be disposed of following the processes prescribed in Chapter 13 - Media and IT equipment Management, Decommissioning and Disposal.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
11.8.12.C.02	Decommissioning and Disposal	Any storage devices, drums, cartridge memory chips or other components that may contain data or copies of documents SHOULD be disposed of following the processes prescribed in Chapter 13 - Media and IT equipment Management, Decommissioning and Disposal.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
11.8.13.C.01	Logging multifunction device use	Use of MFDs for printing, scanning, and copying purposes SHOULD be centrally logged.	Functional	Intersects With	Multi-Function Devices (MFD)	AST-23	Mechanisms exist to securely configure Multi-Function Devices (MFD) according to industry-recognized secure practices for the type of device.	5	
12.1.30.C.01	Evaluated product selection preference order	Agencies MUST select products in the following order of preference: a protection profile (PP) evaluated product; products having completed an evaluation through the AISEP or recognised under the Common Criteria Recognition Arrangement (CCRA); products in evaluation in the AISEP; products in evaluation in a scheme where the outcome will be recognised by the GCSB when the evaluation is complete; or If products do not fall within any of these categories, contact the GCSB.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	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	
12.1.30.C.02	Evaluated product selection preference order	When choosing a product, agencies MUST document the justification for any decision to choose a product that is still in evaluation and accept any security risk introduced by the use of such a product.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to proactively govern Technology Assets, Applications and/or Services (TAAS) by: (1) Defining technical security, compliance and resilience requirements; and	5	
12.1.30.C.03	Evaluated product selection preference order	Agencies SHOULD select products in the following order of preference: a protection profile (PP) evaluated product; products having completed an evaluation through the AISEP or recognised under the Common Criteria Recognition Arrangement (CCRA); products in evaluation in the AISEP; products in evaluation in a scheme where the outcome will be recognised by the GCSB when the evaluation is complete; or If products do not fall within any of these categories, normal selection criteria (such as functionality and security) will apply.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	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	
12.1.31.C.01	Evaluated product selection	Agencies SHOULD select products that have their desired security functionality within the scope of the products evaluation and are applicable to the agency's intended environment.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of 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	
12.1.32.C.01	Product specific requirements	Agencies MUST check consumer guides for products, where available, to determine any product specific requirements.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to proactively govern Technology Assets, Applications and/or Services (TAAS) by: (1) Defining technical security, compliance and resilience requirements; and	5	
12.1.32.C.01	Product specific requirements	Agencies MUST check consumer guides for products, where available, to determine any product specific requirements.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
12.1.32.C.01	Product specific requirements	Agencies MUST check consumer guides for products, where available, to determine any product specific requirements.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of 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	
12.1.32.C.02	Product specific requirements	Where product specific requirements exist in a consumer guide, agencies MUST comply with the requirements outlined in the consumer guide.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to proactively govern Technology Assets, Applications and/or Services (TAAS) by: (1) Defining technical security, compliance and resilience requirements; and	5	
12.1.32.C.02	Product specific requirements	Where product specific requirements exist in a consumer guide, agencies MUST comply with the requirements outlined in the consumer guide.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
12.1.32.C.02	Product specific requirements	Where product specific requirements exist in a consumer guide, agencies MUST comply with the requirements outlined in the consumer guide.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of 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	
12.1.32.C.03	Product specific requirements	Agencies selecting high assurance products and HACE MUST contact the GCSB and comply with any product specific requirements, before any purchase is made.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to proactively govern Technology Assets, Applications and/or Services (TAAS) by: (1) Defining technical security, compliance and resilience requirements; and	5	
12.1.32.C.03	Product specific requirements	Agencies selecting high assurance products and HACE MUST contact the GCSB and comply with any product specific requirements, before any purchase is made.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
12.1.32.C.03	Product specific requirements	Agencies selecting high assurance products and HACE MUST contact the GCSB and comply with any product specific requirements, before any purchase is made.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of 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	
12.1.33.C.01	Sourcing non-evaluated software	Agencies SHOULD: obtain software from verifiable sources and verify its integrity using vendor supplied checksums; and validate the softwares interaction with the operating systems and network within a test environment prior to use on operational systems.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of 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	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
12.1.34.C.01	Delivery of evaluated products	Agencies procuring high assurance products and HACE MUST contact the GCSB and comply with any product specific delivery procedures.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of 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	
12.1.34.C.02	Delivery of evaluated products	Agencies SHOULD ensure that products are delivered in a manner consistent with any delivery procedures defined in associated documentation.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of 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	
12.1.35.C.01	Delivery of non-evaluated products	Agencies SHOULD ensure that products purchased without the delivery assurances provided through the use of formally evaluated procedures are delivered in a manner that provides confidence that they receive the product that they expect to receive in an unaltered state, including checking: any labelling changes; any damage; and any signs of tampering.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of 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	
12.1.36.C.01	Leasing arrangements	Agencies SHOULD ensure that leasing agreements for IT equipment takes into account the: difficulties that could be encountered when the equipment needs maintenance; control of remote maintenance, software updates and fault diagnosis; if the equipment can be easily sanitised prior to its return; and the possible requirement for destruction if sanitisation cannot be performed.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of 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	
12.1.37.C.01	Ongoing maintenance of assurance	Agencies SHOULD choose products from developers that have made a commitment to the ongoing maintenance of the assurance of their product.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of 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	
12.2.5.C.01	Installation and configuration of evaluated products	Agencies MUST ensure that high assurance products and HACE are installed, configured, operated and administered in accordance with all product specific policy.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
12.2.5.C.02	Installation and configuration of evaluated products	Agencies SHOULD install, configure, operate and administer evaluated products in accordance with available documentation resulting from the products evaluation.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
12.2.6.C.01	Use of evaluated products in unevaluated configurations	Agencies wishing to use a product in an unevaluated configuration MUST undertake a security risk assessment including: the necessity of the unevaluated configuration; testing of the unevaluated configuration; and the environment in which the unevaluated product is to be used.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
12.2.6.C.02	Use of evaluated products in unevaluated configurations	High assurance products and HACE MUST NOT be used in unevaluated configurations.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
12.3.4.C.01	Classifying IT equipment	Agencies MUST classify IT equipment based on the highest classification of information the equipment and any associated media within the equipment, are approved for processing, storing or communicating.	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
12.3.4.C.01	Classifying IT equipment	Agencies MUST classify IT equipment based on the highest classification of information the equipment and any associated media within the equipment, are approved for processing, storing or communicating.	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
12.3.5.C.01	Labelling IT equipment	Agencies MUST clearly label all IT equipment capable of storing or processing classified information, with the exception of HACE, with the appropriate protective marking.	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
12.3.5.C.01	Labelling IT equipment	Agencies MUST clearly label all IT equipment capable of storing or processing classified information, with the exception of HACE, with the appropriate protective marking.	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
12.3.5.C.02	Labelling IT equipment	Agencies MUST clearly label all IT equipment in data centres or computer rooms with an asset identification and the level of classification to which that equipment has been accredited.	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
12.3.5.C.02	Labelling IT equipment	Agencies MUST clearly label all IT equipment in data centres or computer rooms with an asset identification and the level of classification to which that equipment has been accredited.	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
12.3.6.C.01	Labelling high assurance products	Agencies MUST NOT have any non-essential labels applied to external surfaces of high assurance products.	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
12.3.6.C.01	Labelling high assurance products	Agencies MUST NOT have any non-essential labels applied to external surfaces of high assurance products.	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
12.3.7.C.01	Labelling HACE	Agencies SHOULD seek GCSB authorisation before applying labels to external surfaces of HACE.	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
12.3.7.C.01	Labelling HACE	Agencies SHOULD seek GCSB authorisation before applying labels to external surfaces of HACE.	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
12.4.3.C.01	Vulnerabilities and patch availability awareness	Agencies SHOULD monitor relevant sources for information about new vulnerabilities and security patches for software and IT equipment used by the agency.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of 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	
12.4.4.C.01	Patching vulnerabilities in products	Agencies MUST apply all critical security patches as soon as possible and within two (2) days of the release of the patch or update.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of 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	
12.4.4.C.02	Patching vulnerabilities in products	Agencies MUST implement a patch management strategy, including an evaluation or testing process.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of 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	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
12.4.4.C.03	Patching vulnerabilities in products	Agencies MUST NOT patch high assurance products or HACE without the patch being approved by the GCSB.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of 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	
12.4.4.C.04	Patching vulnerabilities in products	Agencies SHOULD apply all critical security patches as soon as possible and preferably within two (2) days of the release of the patch or update.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of 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	
12.4.4.C.05	Patching vulnerabilities in products	Agencies SHOULD apply all non-critical security patches as soon as possible.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of 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	
12.4.4.C.06	Patching vulnerabilities in products	Agencies SHOULD ensure that security patches are applied through a vendor recommended patch or upgrade process.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of 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	
12.4.5.C.01	When security patches are not available	Where known vulnerabilities cannot be patched, or security patches are not available, agencies SHOULD implement: controls to resolve the vulnerability such as: disable the functionality associated with the vulnerability though product configuration; ask the vendor for an alternative method of managing the vulnerability; install a version of the product that does not have the identified vulnerability; install a different product with a more responsive vendor; or engage a software developer to correct the software. controls to prevent exploitation of the vulnerability including: apply external input sanitisation (if an input triggers the exploit); apply filtering or verification on the software output (if the exploit relates to an information disclosure); apply additional access controls that prevent access to the vulnerability; or configure firewall rules to limit access to the vulnerable software. controls to contain the exploit including: apply firewall rules limiting outward traffic that is likely in the event of an exploitation; apply mandatory access control preventing the execution of exploitation code; or set file system permissions preventing exploitation code from being written to disk; allow and deny listing to prevent code execution; and controls to detect attacks including: deploy an IDS; monitor logging alerts; or use other mechanisms as appropriate for the detection of exploits using the known vulnerability.	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
12.4.5.C.01	When security patches are not available	Where known vulnerabilities cannot be patched, or security patches are not available, agencies SHOULD implement: controls to resolve the vulnerability such as: disable the functionality associated with the vulnerability though product configuration; ask the vendor for an alternative method of managing the vulnerability; install a version of the product that does not have the identified vulnerability; install a different product with a more responsive vendor; or engage a software developer to correct the software. controls to prevent exploitation of the vulnerability including: apply external input sanitisation (if an input triggers the exploit); apply filtering or verification on the software output (if the exploit relates to an information disclosure); apply additional access controls that prevent access to the vulnerability; or configure firewall rules to limit access to the vulnerable software. controls to contain the exploit including: apply firewall rules limiting outward traffic that is likely in the event of an exploitation; apply mandatory access control preventing the execution of exploitation code; or set file system permissions preventing exploitation code from being written to disk; allow and deny listing to prevent code execution; and controls to detect attacks including: deploy an IDS; monitor logging alerts; or use other mechanisms as appropriate for the detection of exploits using the known vulnerability.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of 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	
12.4.6.C.01	Firmware updates	Agencies MUST ensure that any firmware updates are performed in a manner that verifies the integrity and authenticity of the source and of the updating process or updating utility.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of 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	
12.4.7.C.01	Unsupported products	Agencies SHOULD assess the security risk of continued use of software or IT equipment when a cessation date for support is announced or when the product is no longer supported by the developer.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of 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	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
12.4.7.C.01	Unsupported products	Agencies SHOULD assess the security risk of continued use of software or IT equipment when a cessation date for support is announced or when the product is no longer supported by the developer.	Functional	Intersects With	Unsupported Technology Assets, Applications and/or Services (TAAS)	TDA-17	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs.	5	
12.5.3.C.01	Maintenance and repairs	Agencies MUST seek GCSB approval before undertaking any repairs to high assurance products or HACE.	Functional	Subset Of	Maintenance Operations	MNT-01	Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise.	10	
12.5.3.C.01	Maintenance and repairs	Agencies MUST seek GCSB approval before undertaking any repairs to high assurance products or HACE.	Functional	Intersects With	Controlled Maintenance	MNT-02	Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application and/or Service (TAAS).	5	
12.5.3.C.02	Maintenance and repairs	Maintenance and repairs of IT equipment containing media SHOULD be carried out on-site by an appropriately cleared technician.	Functional	Subset Of	Maintenance Operations	MNT-01	Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise.	10	
12.5.3.C.02	Maintenance and repairs	Maintenance and repairs of IT equipment containing media SHOULD be carried out on-site by an appropriately cleared technician.	Functional	Intersects With	Controlled Maintenance	MNT-02	Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application and/or Service (TAAS).	5	
12.5.4.C.01	Maintenance and repairs by an uncleared technician	If an uncleared technician is used to undertake maintenance or repairs of IT equipment, the technician MUST be escorted by someone who: is appropriately cleared and briefed; takes due care to ensure that classified information is not disclosed; takes all responsible measures to ensure the integrity of the equipment; and has the authority to direct the technician.	Functional	Intersects With	Maintenance Personnel Without Appropriate Access	MNT-06.1	Mechanisms exist to ensure the risks associated with maintenance personnel who do not have appropriate access authorizations, clearances or formal access approvals are appropriately mitigated.	5	
12.5.4.C.02	Maintenance and repairs by an uncleared technician	If an uncleared technician is used to undertake maintenance or repairs of IT equipment, agencies SHOULD sanitise and reclassify or declassify the equipment and associated media before maintenance or repair work is undertaken.	Functional	Intersects With	Maintenance Personnel Without Appropriate Access	MNT-06.1	Mechanisms exist to ensure the risks associated with maintenance personnel who do not have appropriate access authorizations, clearances or formal access approvals are appropriately mitigated.	5	
12.5.4.C.03	Maintenance and repairs by an uncleared technician	Agencies SHOULD ensure that the ratio of escorts to uncleared technicians allows for appropriate oversight of all activities.	Functional	Intersects With	Maintenance Personnel Without Appropriate Access	MNT-06.1	Mechanisms exist to ensure the risks associated with maintenance personnel who do not have appropriate access authorizations, clearances or formal access approvals are appropriately mitigated.	5	
12.5.4.C.04	Maintenance and repairs by an uncleared technician	If an uncleared technician is used to undertake maintenance or repairs of IT equipment, the technician SHOULD be escorted by someone who is sufficiently familiar with the product to understand the work being performed.	Functional	Intersects With	Maintenance Personnel Without Appropriate Access	MNT-06.1	Mechanisms exist to ensure the risks associated with maintenance personnel who do not have appropriate access authorizations, clearances or formal access approvals are appropriately mitigated.	5	
12.5.5.C.01	Off-site maintenance and repairs	Agencies having IT equipment maintained or repaired off-site MUST ensure that the physical transfer, processing and storage requirements are appropriate for the classification of the product and are maintained at all times.	Functional	Intersects With	Field Maintenance	MNT-08	Mechanisms exist to securely conduct field maintenance on geographically deployed assets.	5	
12.5.5.C.01	Off-site maintenance and repairs	Agencies having IT equipment maintained or repaired off-site MUST ensure that the physical transfer, processing and storage requirements are appropriate for the classification of the product and are maintained at all times.	Functional	Intersects With	Off-Site Maintenance	MNT-09	Mechanisms exist to ensure off-site maintenance activities are conducted securely and the asset(s) undergoing maintenance actions are secured during physical transfer and storage while off-site.	5	
12.5.6.C.01	Maintenance and repair of IT equipment from secure areas	Offsite repairs and maintenance SHOULD treat all equipment in accordance with the requirements for the highest classification of information processed, stored or communicated in the area that the equipment will be returned to.	Functional	Subset Of	Maintenance Operations	MNT-01	Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise.	10	
12.5.6.C.01	Maintenance and repair of IT equipment from secure areas	Offsite repairs and maintenance SHOULD treat all equipment in accordance with the requirements for the highest classification of information processed, stored or communicated in the area that the equipment will be returned to.	Functional	Intersects With	Controlled Maintenance	MNT-02	Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application and/or Service (TAAS).	5	
12.5.6.C.02	Maintenance and repair of IT equipment from secure areas	Agencies SHOULD conduct or arrange to have technical inspections conducted on all equipment returned to the secure area after maintenance or repair.	Functional	Subset Of	Maintenance Operations	MNT-01	Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise.	10	
12.5.6.C.02	Maintenance and repair of IT equipment from secure areas	Agencies SHOULD conduct or arrange to have technical inspections conducted on all equipment returned to the secure area after maintenance or repair.	Functional	Intersects With	Controlled Maintenance	MNT-02	Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application and/or Service (TAAS).	5	
12.6.4.C.01	Sanitisation or destruction of IT equipment	Agencies MUST sanitise or destroy, then declassify, IT equipment containing any media before disposal.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
12.6.4.C.02	Sanitisation or destruction of IT equipment	IT equipment and associated media that have processed or stored NZEO information, and cannot be sanitised, MUST be returned to New Zealand for sanitisation or destruction, declassification and disposal.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
12.6.5.C.01	Disposal of IT equipment	Agencies MUST have a documented process for the disposal of IT equipment.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
12.6.5.C.02	Disposal of IT equipment	Agencies MUST contact the GCSB and comply with any requirements for the disposal of high assurance products.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
12.6.5.C.03	Disposal of IT equipment	Agencies MUST contact the GCSB and comply with any requirements for the disposal of HACE.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
12.6.5.C.04	Disposal of IT equipment	Agencies MUST contact GCSB and comply with any requirements for the disposal of TEMPEST rated IT equipment or if the equipment is non-functional.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
12.6.5.C.05	Disposal of IT equipment	Agencies MUST formally sanitise and then authorise the disposal of IT equipment, or waste, into the public domain.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
12.6.5.C.05	Disposal of IT equipment	Agencies MUST formally sanitise and then authorise the disposal of IT equipment, or waste, into the public domain.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
12.6.6.C.01	Sanitising printer cartridges and copier drums	Agencies MUST print at least three pages of random text with no blank areas on each colour printer cartridge with an integrated drum or separate copier drum.	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
12.6.6.C.02	Sanitising printer cartridges and copier drums	Agencies SHOULD print at least three pages of random text with no blank areas on each colour printer cartridge with an integrated drum or separate copier drum.	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
12.6.7.C.01	Destroying printer cartridges and copier drums	Agencies unable to sanitise printer cartridges with integrated copier drums or discrete copier drums, MUST destroy the cartridge or drum.	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
12.6.7.C.02	Destroying printer cartridges and copier drums	Agencies unable to sanitise printer cartridges with integrated copier drums or discrete copier drums, SHOULD destroy the cartridge or drum.	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
12.6.8.C.01	Disposal of televisions and monitors	Agencies MUST visually inspect video screens by turning up the brightness to the maximum level to determine if any classified information has been burnt into or persists on the screen, before redeployment or disposal.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
12.6.9.C.01	Sanitising televisions and monitors	Agencies MUST attempt to sanitise video screens with minor burn-in or image persistence by displaying a solid white image on the screen for an extended period of time. If burn-in cannot be corrected the screen MUST be processed through an approved destruction facility.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
12.6.10.C.01	LCD/LED, plasma and non-CRT monitor types	Because of the risks that data can be recovered from monitors, it is essential that any redeployment or disposal of monitors MUST follow the guidance in the NZISM.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
12.7.14.C.01	Risk Management	Agencies SHOULD incorporate the consideration of supply chain risks into an organisation-wide risk assessment and management process.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
12.7.14.C.01	Risk Management	Agencies SHOULD incorporate the consideration of supply chain risks into an organisation-wide risk assessment and management process.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	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	
12.7.14.C.02	Risk Management	Agencies SHOULD monitor supply chain risks on an ongoing basis and adjust mitigations and controls appropriately.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
12.7.14.C.02	Risk Management	Agencies SHOULD monitor supply chain risks on an ongoing basis and adjust mitigations and controls appropriately.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	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	
12.7.14.C.03	Risk Management	Agencies SHOULD follow the Government Rules of Procurement.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
12.7.14.C.03	Risk Management	Agencies SHOULD follow the Government Rules of Procurement.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	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	
12.7.15.C.01	Contractor or Supplier Capability	Agencies SHOULD require tenderers and contractors to provide information: identifying any restrictions on the disclosure, transfer or use of technology arising out of export controls or security arrangements; and demonstrating that their supply chains comply with the security of supply requirements set out in the contract documents.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
12.7.15.C.01	Contractor or Supplier Capability	Agencies SHOULD require tenderers and contractors to provide information: identifying any restrictions on the disclosure, transfer or use of technology arising out of export controls or security arrangements; and demonstrating that their supply chains comply with the security of supply requirements set out in the contract documents.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	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	
12.7.15.C.02	Contractor or Supplier Capability	Agencies SHOULD request information from contractors and subcontractors to assess their ability to protect information.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
12.7.15.C.02	Contractor or Supplier Capability	Agencies SHOULD request information from contractors and subcontractors to assess their ability to protect information.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	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	
12.7.16.C.01	Security of Information	Agencies MUST include contractual obligations on all contractors and subcontractors to safeguard information throughout the tendering and contracting procedure.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
12.7.16.C.01	Security of Information	Agencies MUST include contractual obligations on all contractors and subcontractors to safeguard information throughout the tendering and contracting procedure.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	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	
12.7.16.C.02	Security of Information	Agencies SHOULD include contractual obligations to safeguard information throughout the tendering and contracting procedure.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
12.7.16.C.02	Security of Information	Agencies SHOULD include contractual obligations to safeguard information throughout the tendering and contracting procedure.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	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	
12.7.16.C.03	Security of Information	Agencies SHOULD reject contractors and subcontractors where they do not possess the necessary reliability to exclude risks to national security; or have breached obligations relating to security of information during a previous contract in circumstances amounting to grave misconduct.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
12.7.16.C.03	Security of Information	Agencies SHOULD reject contractors and subcontractors where they do not possess the necessary reliability to exclude risks to national security; or have breached obligations relating to security of information during a previous contract in circumstances amounting to grave misconduct.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	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	
12.7.17.C.01	Continuity of Supply	Agencies SHOULD ensure that changes in their supply chain during the performance of the contract will not adversely affect the continuity of supply requirements.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
12.7.17.C.01	Continuity of Supply	Agencies SHOULD ensure that changes in their supply chain during the performance of the contract will not adversely affect the continuity of supply requirements.	Functional	Intersects With	Third-Party Criticality Assessments	TPM-02	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	
12.7.17.C.01	Continuity of Supply	Agencies SHOULD ensure that changes in their supply chain during the performance of the contract will not adversely affect the continuity of supply requirements.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	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	
12.7.18.C.01	Product Assurance	Agencies MUST require suppliers and contractors to provide the provenance of any products or equipment.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
12.7.18.C.01	Product Assurance	Agencies MUST require suppliers and contractors to provide the provenance of any products or equipment.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	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	
12.7.18.C.02	Product Assurance	Agencies SHOULD require suppliers and contractors to provide the provenance of any products or equipment.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
12.7.18.C.02	Product Assurance	Agencies SHOULD require suppliers and contractors to provide the provenance of any products or equipment.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	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	
12.7.19.C.01	Security validation	Agencies SHOULD validate the security of the equipment against security performance, capability and functionality requirements.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
12.7.19.C.01	Security validation	Agencies SHOULD validate the security of the equipment against security performance, capability and functionality requirements.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	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	
12.7.19.C.02	Security validation	Where deficiencies in security performance, capability and functionality are identified, agencies SHOULD implement additional risk mitigation measures.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
12.7.19.C.02	Security validation	Where deficiencies in security performance, capability and functionality are identified, agencies SHOULD implement additional risk mitigation measures.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	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	
12.7.20.C.01	Pre-Installation Tests and Checks	Agencies MUST consult with the GCSB on pre-installation, security verification and related tests before the equipment is used in an operational system.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
12.7.20.C.01	Pre-Installation Tests and Checks	Agencies MUST consult with the GCSB on pre-installation, security verification and related tests before the equipment is used in an operational system.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	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	
12.7.20.C.02	Pre-Installation Tests and Checks	Agencies SHOULD inspect equipment on receipt for any obvious signs of tampering, relabelling or damage.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
12.7.20.C.02	Pre-Installation Tests and Checks	Agencies SHOULD inspect equipment on receipt for any obvious signs of tampering, relabelling or damage.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	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	
12.7.20.C.03	Pre-Installation Tests and Checks	Agencies SHOULD inspect equipment on receipt and test the operation before installation.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
12.7.20.C.03	Pre-Installation Tests and Checks	Agencies SHOULD inspect equipment on receipt and test the operation before installation.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	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	
12.7.20.C.04	Pre-Installation Tests and Checks	Agencies SHOULD conduct installation verification and related tests before the equipment is used in an operational system.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
12.7.20.C.04	Pre-Installation Tests and Checks	Agencies SHOULD conduct installation verification and related tests before the equipment is used in an operational system.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	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	
12.7.20.C.05	Pre-Installation Tests and Checks	Where any software, firmware or other forms of programme code are required for the initialisation, operation, servicing or maintenance of the equipment, malware checks SHOULD be conducted before the equipment is installed in an operational system.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
12.7.20.C.05	Pre-Installation Tests and Checks	Where any software, firmware or other forms of programme code are required for the initialisation, operation, servicing or maintenance of the equipment, malware checks SHOULD be conducted before the equipment is installed in an operational system.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	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	
12.7.21.C.01	Equipment Servicing	For equipment that is expected to have an extended operational life in a critical system, and in the event that the supplier is no longer able to supply these, agencies SHOULD provide for the acquisition of: necessary licences; information to produce spare parts, components, assemblies; testing equipment; and technical assistance agreements.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
12.7.21.C.01	Equipment Servicing	For equipment that is expected to have an extended operational life in a critical system, and in the event that the supplier is no longer able to supply these, agencies SHOULD provide for the acquisition of: necessary licences; information to produce spare parts, components, assemblies; testing equipment; and technical assistance agreements.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	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	
13.1.9.C.01	Agency Policy	When the Information System reaches the end of its service life in an organisation, policy and procedures SHOULD be in place to ensure secure decommissioning and transfer or disposal, in order to satisfy corporate, legal and statutory requirements.	Functional	Intersects With	Decommissioning	AST-30	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are properly decommissioned so that data is properly transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	
13.1.10.C.01	Migration plan	Agencies SHOULD undertake a risk assessment with consideration given to proportionality in respect of: scale and impact of the processes; data; users; licences; usage agreements; and service to be migrated or decommissioned.	Functional	Intersects With	Decommissioning	AST-30	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are properly decommissioned so that data is properly transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
13.1.10.C.02	Migration plan	The risk assessment SHOULD include the following elements: Evaluation of the applications inventory and identification of any redundancies; Identification of data owners and key stakeholders; Identification of types of information (Active or Inactive) processed and stored; Identification of software and other (including non-transferable) licences; Identification of access rights to be transferred or cancelled; Identification of any emanation control equipment or security enhancements; Consideration of short and long term reporting requirements; Assessment of equipment and hardware for redeployment or disposal; Identification of any cloud-based data and services; and User re-training.	Functional	Intersects With	Decommissioning	AST-30	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are properly decommissioned so that data is properly transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	
13.1.10.C.03	Migration plan	Agencies SHOULD consider the need for a Privacy Impact Assessment.	Functional	Intersects With	Decommissioning	AST-30	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are properly decommissioned so that data is properly transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	
13.1.10.C.04	Migration plan	Agencies SHOULD identify relevant service and legal agreements and arrange for their termination.	Functional	Intersects With	Decommissioning	AST-30	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are properly decommissioned so that data is properly transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	
13.1.11.C.01	Decommissioning plan	The decommissioning plan will be based on the migration plan and SHOULD incorporate the following elements: An impact analysis; Issue of notification to service providers, users and customers; Issue of notification of decommissioning to all relevant interfaces and interconnections; Timeframe, plan and schedule; Data integrity and validation checks before archiving; Transfer or redeployment of equipment and other assets; Transfer or cancellation of licences; Removal of redundant equipment and software; Removal of redundant cables and termination equipment; Removal of any emanation control equipment or security enhancements; Return or safe disposal of any emanation control equipment or security enhancements; Updates to systems configurations (switches, firewalls etc.); Equipment and media sanitisation including any cloud-based data & services(discussed later in this chapter); Equipment and media disposal (discussed later in this chapter); Any legal considerations for supply or service contract terminations; Asset register updates; and Retraining for, or redeployment of, support staff.	Functional	Intersects With	Decommissioning	AST-30	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are properly decommissioned so that data is properly transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	
13.1.12.C.01	Archiving	Agencies SHOULD identify data retention policies, regulation and legislation.	Functional	Intersects With	Decommissioning	AST-30	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are properly decommissioned so that data is properly transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	
13.1.12.C.02	Archiving	Agencies SHOULD ensure adequate system documentation is archived.	Functional	Intersects With	Decommissioning	AST-30	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are properly decommissioned so that data is properly transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	
13.1.12.C.03	Archiving	Agencies SHOULD archive essential software, system logic, system documentation and other system data to allow information to be recovered from archive.	Functional	Intersects With	Decommissioning	AST-30	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are properly decommissioned so that data is properly transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	
13.1.13.C.01	Audit and Final signoff	The agency's Accreditation Authority SHOULD confirm IA compliance on decommissioning and disposal.	Functional	Intersects With	Decommissioning	AST-30	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are properly decommissioned so that data is properly transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	
13.1.13.C.02	Audit and Final signoff	The agency's Accreditation Authority SHOULD confirm secure equipment and media disposal.	Functional	Intersects With	Decommissioning	AST-30	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are properly decommissioned so that data is properly transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	
13.1.13.C.03	Audit and Final signoff	The agency's Accreditation Authority SHOULD confirm asset register updates.	Functional	Intersects With	Decommissioning	AST-30	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are properly decommissioned so that data is properly transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	
13.1.13.C.04	Audit and Final signoff	Once all security relevant activities associated with decommissioning and disposal have been completed and verified, a Security Decommissioning Compliance Certificate SHOULD be issued by the agency's Accreditation Authority.	Functional	Intersects With	Decommissioning	AST-30	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are properly decommissioned so that data is properly transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	
13.1.14.C.01	Final Review	Agencies SHOULD undertake a post-decommissioning review.	Functional	Intersects With	Decommissioning	AST-30	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are properly decommissioned so that data is properly transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	
13.2.6.C.01	Reclassification and declassification procedures	Agencies MUST document procedures for the reclassification and declassification of media.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
13.2.7.C.01	Classifying media storing information	Agencies MUST classify media to the highest classification of data stored on the media.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
13.2.8.C.01	Classifying media connected to systems of higher classifications	Agencies MUST classify any media connected to a system of a higher classification at the higher system classification until confirmed not to be the case.	Functional	Intersects With	Highest Classification Level	DCH-02.1	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	
13.2.9.C.01	Classifying media below that of the system	Agencies intending to classify media below the classification of the system to which it is connected to MUST ensure that: the media is read-only; the media is inserted into a read-only device; or the system has a mechanism through which read-only access can be assured such as approved data diodes, write-blockers or similar infrastructure.	Functional	Intersects With	Highest Classification Level	DCH-02.1	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	
13.2.10.C.01	Reclassifying media to a lower classification	Agencies wishing to reclassify media to a lower classification MUST ensure that: a formal decision is made to reclassify, or redeploy the media; and the reclassification of all information on the media has been approved by the originator, or the media has been appropriately sanitised or destroyed.	Functional	Intersects With	Data Reclassification	DCH-11	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	
13.2.11.C.01	Reclassifying media to a higher classification	Agencies MUST reclassify media if: information copied onto the media is of a higher classification; or information contained on the media is subjected to a classification upgrade.	Functional	Intersects With	Data Reclassification	DCH-11	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	
13.2.12.C.01	Labelling media	Agencies MUST label media with a marking that indicates the maximum classification and any endorsements applicable to the information stored.	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
13.2.12.C.02	Labelling media	Agencies MUST ensure that the classification of all media is easily visually identifiable.	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
13.2.12.C.03	Labelling media	When using non-textual (colour, symbol) protective markings for operational security reasons, agencies MUST document the labelling scheme and train personnel appropriately.	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
13.2.12.C.04	Labelling media	Agencies SHOULD label media with a marking that indicates the maximum classification and any endorsements applicable to the information stored.	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
13.2.13.C.01	Labelling sanitised media	Agencies MUST label non-volatile media that has been sanitised and reclassified for redeployment with a notice similar to: Warning: media has been sanitised and reclassified from [classification] to [classification]. Further lowering of classification only via destruction.	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
13.2.14.C.01	Registering media	Agencies MUST register all media with a unique identifier in an appropriate register.	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
13.2.14.C.02	Registering media	Agencies SHOULD register all media with a unique identifier in an appropriate register.	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
13.3.4.C.01	Using media with systems	Agencies MUST NOT use media containing classified information with a system that has a classification lower than the classification of the media.	Functional	Intersects With	Media Use	DCH-10	Mechanisms exist to restrict the use of types of digital media on systems or system components.	5	
13.3.4.C.01	Using media with systems	Agencies MUST NOT use media containing classified information with a system that has a classification lower than the classification of the media.	Functional	Intersects With	Limitations on Use	DCH-10.1	Mechanisms exist to restrict the use and distribution of sensitive and/or regulated data.	5	
13.3.5.C.01	Storage of media	Agencies MUST ensure that storage facilities for media containing classified information meets the minimum physical security storage requirements as specified in the PSR Policy Framework - Physical Security.	Functional	Intersects With	Media Storage	DCH-06	Mechanisms exist to: (1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and (2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures.	5	
13.3.6.C.01	Connecting media to systems	Agencies MUST disable any automatic execution features within operating systems for connectable devices and media.	Functional	Intersects With	Removable Media Security	DCH-12	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	5	
13.3.6.C.02	Connecting media to systems	Agencies MUST prevent unauthorised media from connecting to a system via the use of: device access control software; seals; physical means; or other methods approved by the Accreditation Authority.	Functional	Intersects With	Removable Media Security	DCH-12	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	5	
13.3.6.C.03	Connecting media to systems	When writable media is connected to a writable communications port or device, agencies SHOULD implement controls to prevent the unintended writing of data to the media.	Functional	Intersects With	Removable Media Security	DCH-12	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	5	
13.3.7.C.01	IEEE 1394 (FIREWIRE) interface connections	Agencies MUST disable IEEE 1394 interfaces.	Functional	Intersects With	Portable Storage Devices	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.	5	
13.3.7.C.02	IEEE 1394 (FIREWIRE) interface connections	Agencies SHOULD disable IEEE 1394 interfaces.	Functional	Intersects With	Portable Storage Devices	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.	5	
13.3.8.C.01	Transferring media	Agencies MUST ensure that processes for transferring media containing classified information meets the minimum physical transfer requirements as specified in the PSR.	Functional	Intersects With	Portable Storage Devices	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.	5	
13.3.8.C.02	Transferring media	Agencies SHOULD encrypt data stored on media with at least an Approved Cryptographic Algorithm (See Section 17.2 - Approved Cryptographic Algorithms) if it is to be transferred to another area or location.	Functional	Intersects With	Portable Storage Devices	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.	5	
13.3.9.C.01	Using media for data transfers	Data transfers between systems of different classification SHOULD be logged in an auditable log or register.	Functional	Intersects With	Portable Storage Devices	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.	5	
13.3.9.C.02	Using media for data transfers	Agencies transferring data manually between two systems of different security domains or classifications SHOULD NOT use rewriteable media.	Functional	Intersects With	Portable Storage Devices	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.	5	
13.3.10.C.01	Media in secure areas	Agencies MUST NOT permit any media that uses external interface connections within a TOP SECRET area without prior written approval from the Accreditation Authority.	Functional	Intersects With	Removable Media Security	DCH-12	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	5	
13.3.10.C.01	Media in secure areas	Agencies MUST NOT permit any media that uses external interface connections within a TOP SECRET area without prior written approval from the Accreditation Authority.	Functional	Intersects With	Portable Storage Devices	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.	5	
13.4.9.C.01	Sanitisation procedures	Agencies MUST document conditions and procedures for the sanitisation of media and IT Equipment.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
13.4.10.C.01	Media that cannot be sanitised	Agencies MUST destroy the following media types prior to disposal, as they cannot be effectively sanitised: microfiche; microfilm; optical discs; printer ribbons and the impact surface facing the platen; programmable read-only memory (PROM, EPROM, EEPROM); flash memory and solid state or hybrid data storage devices; read-only memory; and faulty magnetic media that cannot be successfully sanitised.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
13.4.11.C.01	Volatile media sanitisation	Agencies MUST sanitise volatile media by: overwriting all locations of the media with an arbitrary pattern; followed by a read back for verification; and removing power from the media for at least 10 minutes.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
13.4.12.C.01	Treatment of volatile media following sanitisation	Following sanitisation, volatile media MUST be treated as indicated in the table below. Pre-sanitisation classification / Endorsement Post-sanitisation classification / Endorsement New Zealand Eyes Only (NZEO) Endorsement NZEO TOP SECRET TOP SECRET SECRET SECRET CONFIDENTIAL UNCLASSIFIED RESTRICTED and all lower classifications UNCLASSIFIED	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
13.4.13.C.01	Non-volatile magnetic media sanitisation	Agencies MUST sanitise non-volatile magnetic media by: if pre-2001 or under 15GB: overwriting the media at least three times in its entirety with an arbitrary pattern followed by a read back for verification; or if post-2001 or over 15GB: overwriting the media at least once in its entirety with an arbitrary pattern followed by a read back for verification.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
13.4.13.C.02	Non-volatile magnetic media sanitisation	Agencies MUST boot from separate media to the media being sanitised when undertaking sanitisation.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
13.4.13.C.03	Non-volatile magnetic media sanitisation	Agencies SHOULD reset the host protected area and drive configuration overlay table of non-volatile magnetic hard disks prior to overwriting the media.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
13.4.13.C.04	Non-volatile magnetic media sanitisation	Agencies SHOULD attempt to overwrite the growth defects table (g-list) on non-volatile magnetic hard disks.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
13.4.13.C.05	Non-volatile magnetic media sanitisation	Agencies SHOULD use the ATA security erase command for sanitising non-volatile magnetic hard disks instead of using block overwriting software.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
13.4.14.C.01	Treatment of non-volatile magnetic media following sanitisation	Following sanitisation, non-volatile magnetic media MUST be treated as indicated in the table below. Pre-sanitisation classification Post-sanitisation classification New Zealand Eyes Only (NZEO) Endorsement NZEO TOP SECRET TOP SECRET SECRET SECRET CONFIDENTIAL UNCLASSIFIED RESTRICTED UNCLASSIFIED	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
13.4.15.C.01	Non-volatile EPROM media sanitisation	Agencies MUST sanitise non-volatile EPROM media by erasing as per the manufacturers specification, increasing the specified ultraviolet erasure time by a factor of three, then overwriting the media at least once in its entirety with a pseudo random pattern, followed by a read back for verification.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
13.4.16.C.01	Non-volatile EEPROM media sanitisation	Agencies MUST sanitise non-volatile EEPROM media by overwriting the media at least once in its entirety with a pseudo random pattern, followed by a read back for verification.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
13.4.17.C.01	Treatment of non-volatile EPROM and EEPROM media following sanitisation	Following sanitisation, non-volatile EPROM and EEPROM media MUST be treated as indicated in the table below. Pre-sanitisation classification Post-sanitisation classification New Zealand Eyes Only (NZEO) Endorsement NZEO TOP SECRET TOP SECRET SECRET SECRET CONFIDENTIAL UNCLASSIFIED RESTRICTED UNCLASSIFIED	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
13.4.18.C.01	Non-volatile flash memory & FPGA media sanitisation	Agencies MUST sanitise non-volatile flash memory media by overwriting the media at least twice in its entirety with a pseudo random pattern, followed by a read back for verification.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
13.4.19.C.01	Treatment of non-volatile flash memory & FPCA media following sanitisation	Following sanitisation, non-volatile flash memory media MUST be treated as indicated in the table below. Pre-sanitisation classification Post-sanitisation classification New Zealand Eyes Only (NZEO) Endorsement NZEO TOP SECRET TOP SECRET SECRET SECRET CONFIDENTIAL CONFIDENTIAL RESTRICTED UNCLASSIFIED	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
13.4.19.C.02	Treatment of non-volatile flash memory & FPCA media following sanitisation	Where manufacturer sanitation procedures cannot be determined, items MUST be destroyed.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
13.4.19.C.02	Treatment of non-volatile flash memory & FPCA media following sanitisation	Where manufacturer sanitation procedures cannot be determined, items MUST be destroyed.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
13.4.20.C.01	Sanitising solid state drives	Solid state drives MUST be destroyed before disposal.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
13.4.20.C.02	Sanitising solid state drives	Solid state drives MUST be sanitised using ATA Secure Erase sanitation software before redeployment.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
13.4.20.C.03	Sanitising solid state drives	Solid state drives MUST NOT be redeployed in a lower classification environment.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
13.4.21.C.01	Hybrid Drives	Hybrid drives MUST be treated as solid state drives for sanitisation purposes.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
13.4.22.C.01	Sanitising media and IT Equipment prior to reuse	Agencies SHOULD sanitise all media and IT Equipment prior to reuse at the same or higher classification.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
13.4.23.C.01	Verifying sanitised media and IT Equipment	Agencies SHOULD verify the sanitisation of media and IT Equipment using a different product from the one used to perform the initial sanitisation.	Functional	Intersects With	Equipment Testing	DCH-09.2	Mechanisms exist to test sanitization equipment and procedures to verify that the intended result is achieved.	5	
13.5.22.C.01	Destruction procedures	Agencies MUST document procedures for the destruction of media and IT Equipment.	Functional	Intersects With	System Media Sanitization Documentation	DCH-09.1	Mechanisms exist to supervise, track, document and verify system media sanitization and disposal actions.	5	
13.5.23.C.01	Media and IT Equipment destruction	To destroy media and IT Equipment agencies MUST use at least one of the methods shown in the following table. Item Destruction methods Furnace/ Incinerator Hammer mill Disintegrator Grinder/ Sander Cutting Degausser Magnetic floppy disks Yes Yes Yes No Yes Yes Magnetic hard disks Yes Yes Yes Yes No Yes Magnetic tapes Yes Yes Yes No Yes	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
13.5.24.C.01	Destruction methods for media and IT equipment	Media and IT equipment destruction MUST be performed using approved destruction equipment, facilities and methods.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
13.5.24.C.01	Destruction methods for media and IT equipment	Media and IT equipment destruction MUST be performed using approved destruction equipment, facilities and methods.	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
13.5.24.C.02	Destruction methods for media and IT equipment	Where agencies do not own their own destruction equipment, agencies MUST use an approved destruction facility for media and IT equipment destruction.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
13.5.24.C.02	Destruction methods for media and IT equipment	Where agencies do not own their own destruction equipment, agencies MUST use an approved destruction facility for media and IT equipment destruction.	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
13.5.24.C.03	Destruction methods for media and IT equipment	Where a facility is NOT an approved facility, agencies MUST ensure any incineration equipment is rated for the destruction of electronic waste (WEEE) and the operator is properly authorised or licensed.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
13.5.24.C.03	Destruction methods for media and IT equipment	Where a facility is NOT an approved facility, agencies MUST ensure any incineration equipment is rated for the destruction of electronic waste (WEEE) and the operator is properly authorised or licensed.	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
13.5.24.C.04	Destruction methods for media and IT equipment	Where a facility is NOT an approved facility, agencies MUST ensure processes are in place for the safe handling of electronic waste (WEEE), including any residual material from the destruction process.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
13.5.24.C.04	Destruction methods for media and IT equipment	Where a facility is NOT an approved facility, agencies MUST ensure processes are in place for the safe handling of electronic waste (WEEE), including any residual material from the destruction process.	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
13.5.25.C.01	Storage and handling of media and IT Equipment waste particles	Agencies MUST, at minimum, store and handle the resulting waste for all methods, in accordance with the classification given in the table below. Initial media or IT Equipment classification Screen aperture size particles can pass through Less than or equal to 3mm Treat as Less than or equal to 6mm Treat as TOP SECRET UNCLASSIFIED RESTRICTED SECRET UNCLASSIFIED RESTRICTED CONFIDENTIAL UNCLASSIFIED RESTRICTED RESTRICTED UNCLASSIFIED UNCLASSIFIED Particle size: measured in any direction, should not exceed stated measurement.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
13.5.25.C.01	Storage and handling of media and IT Equipment waste particles	Agencies MUST, at minimum, store and handle the resulting waste for all methods, in accordance with the classification given in the table below. Initial media or IT Equipment classification Screen aperture size particles can pass through Less than or equal to 3mm Treat as Less than or equal to 6mm Treat as TOP SECRET UNCLASSIFIED RESTRICTED SECRET UNCLASSIFIED RESTRICTED CONFIDENTIAL UNCLASSIFIED RESTRICTED RESTRICTED UNCLASSIFIED UNCLASSIFIED Particle size: measured in any direction, should not exceed stated measurement.	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
13.5.26.C.01	Degaussers	Agencies MUST use a degausser of sufficient field strength for the coercivity of the media and IT Equipment.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
13.5.26.C.01	Degaussers	Agencies MUST use a degausser of sufficient field strength for the coercivity of the media and IT Equipment.	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
13.5.26.C.02	Degaussers	Agencies MUST use a degausser which has been evaluated as capable for the magnetic orientation (longitudinal or perpendicular) of the media.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
13.5.26.C.02	Degaussers	Agencies MUST use a degausser which has been evaluated as capable for the magnetic orientation (longitudinal or perpendicular) of the media.	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
13.5.26.C.03	Degaussers	Agencies MUST comply with product specific directions provided by the manufacturers, along with any provided by the GCSB.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
13.5.26.C.03	Degaussers	Agencies MUST comply with product specific directions provided by the manufacturers, along with any provided by the GCSB.	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
13.5.27.C.01	Supervision of destruction	Agencies MUST perform the destruction of media and IT Equipment under the supervision of at least one person cleared to the highest classification of the media or IT Equipment being destroyed.	Functional	Intersects With	System Media Sanitization Documentation	DCH-09.1	Mechanisms exist to supervise, track, document and verify system media sanitization and disposal actions.	5	
13.5.27.C.02	Supervision of destruction	Personnel supervising the destruction of media or IT Equipment MUST: supervise the handling of the media or IT Equipment to the point of destruction; and ensure that the destruction is completed successfully.	Functional	Intersects With	System Media Sanitization Documentation	DCH-09.1	Mechanisms exist to supervise, track, document and verify system media sanitization and disposal actions.	5	
13.5.27.C.03	Supervision of destruction	The Destruction Register SHOULD record: Destruction facility used; Destruction method used; Date of destruction; Operator and witnesses; Media and IT equipment classification; and Media and IT equipment type, characteristics and serial number.	Functional	Intersects With	System Media Sanitization Documentation	DCH-09.1	Mechanisms exist to supervise, track, document and verify system media sanitization and disposal actions.	5	
13.5.28.C.01	Supervision of accountable material destruction	Agencies MUST perform the destruction of accountable material under the supervision of at least two personnel cleared to the highest classification of the media or IT Equipment being destroyed.	Functional	Intersects With	System Media Sanitization Documentation	DCH-09.1	Mechanisms exist to supervise, track, document and verify system media sanitization and disposal actions.	5	
13.5.28.C.02	Supervision of accountable material destruction	Personnel supervising the destruction of accountable media and IT Equipment MUST: supervise the handling of the material to the point of destruction; ensure that the destruction is completed successfully; sign a destruction certificate; and complete the relevant entries in the destruction register.	Functional	Intersects With	System Media Sanitization Documentation	DCH-09.1	Mechanisms exist to supervise, track, document and verify system media sanitization and disposal actions.	5	
13.5.29.C.01	Outsourcing media and IT Equipment destruction	Agencies MUST NOT outsource the supervision and oversight of the destruction of TOP SECRET or NZEO media and IT equipment or other accountable material to a non-government entity or organisation.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
13.5.29.C.01	Outsourcing media and IT Equipment destruction	Agencies MUST NOT outsource the supervision and oversight of the destruction of TOP SECRET or NZEO media and IT equipment or other accountable material to a non-government entity or organisation.	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
13.5.29.C.02	Outsourcing media and IT Equipment destruction	Agencies outsourcing the destruction of media and IT Equipment to a commercial facility MUST use an approved facility and comply with the procedures and instructions in this Chapter.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
13.5.29.C.02	Outsourcing media and IT Equipment destruction	Agencies outsourcing the destruction of media and IT Equipment to a commercial facility MUST use an approved facility and comply with the procedures and instructions in this Chapter.	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
13.5.30.C.01	Transporting media and IT Equipment for offsite destruction	Agencies SHOULD sanitise media and IT Equipment prior to transporting it to an offsite location for destruction.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
13.5.30.C.01	Transporting media and IT Equipment for offsite destruction	Agencies SHOULD sanitise media and IT Equipment prior to transporting it to an offsite location for destruction.	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
13.6.6.C.01	Declassification prior to disposal	Agencies MUST declassify all media and IT equipment prior to disposing of it into the public domain.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
13.6.6.C.02	Declassification prior to disposal	Media and IT equipment that cannot be effectively sanitised or declassified MUST be destroyed and not released into the public domain.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
13.6.7.C.01	Disposal procedures	Agencies MUST document procedures for the disposal of media and IT equipment.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
13.6.8.C.01	Declassifying media	Agencies declassifying media MUST ensure that: the reclassification of all classified information on the media has been approved by the originator, or the media has been appropriately sanitised or destroyed; and formal approval is granted before the media is released into the public domain.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
13.6.9.C.01	Disposal of media	Agencies MUST dispose of media in a manner that does not draw undue attention to its previous classification.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
13.6.10.C.01	New Zealand Eyes Only (NZEO) Materials	Media and IT equipment that has contained NZEO material MUST be sanitised and redeployed or sanitised and destroyed in accordance with the procedures in this chapter.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
13.6.10.C.02	New Zealand Eyes Only (NZEO) Materials	For disposal of all NZEO endorsed materials, an approved destruction facility MUST be used.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
13.6.10.C.03	New Zealand Eyes Only (NZEO) Materials	Media and IT equipment that has contained NZEO material MUST NOT be disposed of via e-recyclers or sold to any third party.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
13.6.11.C.01	Approved Secure Destruction Facilities	Where agencies establish their own disposal/destruction facilities, these facilities MUST be approved by the Director-General GCSB.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
13.6.12.C.01	Use of Approved Secure Destruction Facilities	Agencies MUST use an approved secure disposal/destruction facility for the destruction of media and IT equipment.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
14.1.8.C.01	Developing hardened SOEs	Agencies SHOULD develop a hardened SOE for workstations and servers, covering: removal of unneeded software and operating system components; removal or disabling of unneeded services, ports and BIOS settings; disabling of unused or undesired functionality in software and operating systems; implementation of access controls on relevant objects to limit system users and programs to the minimum access required; installation of antivirus and anti-malware software; installation of software-based firewalls limiting inbound and outbound network connections; configuration of either remote logging or the transfer of local event logs to a central server; and protection of audit and other logs through the use of a one way pipe to reduce likelihood of compromise key transaction records.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
14.1.9.C.01	Maintaining hardened SOEs	Agencies MUST ensure that for all servers and workstations: a technical specification is agreed for each platform with specified controls; a standard configuration created and updated for each operating system type and version; system users do not have the ability to install or disable software without approval; and installed software and operating system patching is up to date.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
14.1.9.C.02	Maintaining hardened SOEs	Agencies SHOULD ensure that for all servers and workstations: malware detection heuristics are set to a high level; malware pattern signatures are checked for updates on at least a daily basis; malware pattern signatures are updated as soon as possible after vendors make them available; all disks and systems are regularly scanned for malicious code; and the use of End Point Agents is considered.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
14.1.9.C.02	Maintaining hardened SOEs	Agencies SHOULD ensure that for all servers and workstations: malware detection heuristics are set to a high level; malware pattern signatures are checked for updates on at least a daily basis; malware pattern signatures are updated as soon as possible after vendors make them available; all disks and systems are regularly scanned for malicious code; and the use of End Point Agents is considered.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
14.1.10.C.01	Default passwords and accounts	Agencies MUST reduce potential vulnerabilities in their SOEs by: removing unused accounts; renaming or deleting default accounts; and replacing default passwords before or during the installation process.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
14.1.10.C.02	Default passwords and accounts	Agencies SHOULD reduce potential vulnerabilities in their SOEs by: removing unused accounts; renaming or deleting default accounts; and replacing default passwords, before or during the installation process.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
14.1.11.C.01	Server separation	Where servers with a high security risk have connectivity to unsecure public networks, agencies SHOULD: use appropriately designed and configured gateways; consider the use of cross-domain solutions; segment networks; maintain effective functional segregation between servers allowing them to operate independently; minimise communications between servers at both the network and file system level as appropriate; and limit system users and programs to the minimum access needed to perform their duties.	Functional	Intersects With	Separate Subnet for Connecting to Different Security Domains	NET-03.8	Mechanisms exist to implement separate network addresses (e.g., different subnets) to connect to systems in different security domains.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
14.1.12.C.01	Characterisation	Agencies SHOULD: characterise all servers whose functions are critical to the agency, and those identified as being at a high security risk of compromise; store the characterisation information securely off the server in a manner that maintains integrity; update the characterisation information after every legitimate change to a system as part of the change control process; as part of the agency's ongoing audit schedule, compare the stored characterisation information against current characterisation information to determine whether a compromise, or a legitimate but incorrectly completed system modification, has occurred; perform the characterisation from a trusted environment rather than the standard operating system wherever possible; and resolve any detected changes in accordance with the agency's information security incident management procedures.	Functional	Intersects With	Endpoint File Integrity Monitoring (FIM)	END-06	Mechanisms exist to utilize File Integrity Monitor (FIM), or similar technologies, to detect and report on unauthorized changes to selected files and configuration settings.	5	
14.1.12.C.02	Characterisation	Agencies SHOULD use an Approved Cryptographic Algorithm to perform cryptographic checksums for characterisation purposes.	Functional	Intersects With	Endpoint File Integrity Monitoring (FIM)	END-06	Mechanisms exist to utilize File Integrity Monitor (FIM), or similar technologies, to detect and report on unauthorized changes to selected files and configuration settings.	5	
14.1.12.C.03	Characterisation	Agencies SHOULD consider characterisations in the context of a BCP or DRP and any related Business Impact Analyses and Risk Assessments.	Functional	Intersects With	Endpoint File Integrity Monitoring (FIM)	END-06	Mechanisms exist to utilize File Integrity Monitor (FIM), or similar technologies, to detect and report on unauthorized changes to selected files and configuration settings.	5	
14.1.13.C.01	Automated outbound connections by software	Agencies SHOULD review all software applications to determine whether they attempt to establish any unauthorised or unplanned external connections.	Functional	Intersects With	External System Connections	NET-05.1	Mechanisms exist to prohibit the direct connection of a sensitive system to an external network without the use of an organization-defined boundary protection device.	5	
14.1.13.C.02	Automated outbound connections by software	If automated outbound connection functionality is included, agencies SHOULD make a business decision to determine whether to permit or deny these connections, including an assessment of the security risks involved in doing so.	Functional	Intersects With	External System Connections	NET-05.1	Mechanisms exist to prohibit the direct connection of a sensitive system to an external network without the use of an organization-defined boundary protection device.	5	
14.1.13.C.03	Automated outbound connections by software	If automated outbound connection functionality is included, agencies SHOULD consider the implementation of Data Loss Prevention (DLP) technologies.	Functional	Intersects With	External System Connections	NET-05.1	Mechanisms exist to prohibit the direct connection of a sensitive system to an external network without the use of an organization-defined boundary protection device.	5	
14.1.14.C.01	Knowledge of software used on systems	Agencies SHOULD limit information that could be disclosed outside the agency about what software, and software versions are installed on their systems.	Functional	Intersects With	Acceptable Discoverable Information	VPM-06.8	Mechanisms exist to define what information is allowed to be discoverable by adversaries and take corrective actions to remediate non-compliant Technology Assets, Applications and/or Services (TAAS).	5	
14.2.4.C.01	Application allow listing	Agencies SHOULD implement application allow listing as part of the SOE for workstations, servers and any other network device.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5	
14.2.5.C.01	System user permissions	Agencies MUST ensure that a system user cannot disable the application allow listing mechanism.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5	
14.2.5.C.02	System user permissions	Agencies SHOULD prevent a system user from running arbitrary executables.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5	
14.2.5.C.03	System user permissions	Agencies SHOULD restrict a system users rights in order to permit them to only execute a specific set of predefined executables as required for them to complete their duties.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5	
14.2.5.C.04	System user permissions	Agencies SHOULD ensure that application allow listing does not replace the antivirus and anti-malware software within a system.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5	
14.2.6.C.01	System administrator permissions	Agencies SHOULD ensure that system administrators are not automatically exempt from application allow list policy.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5	
14.2.7.C.01	Application allow listing configuration	Agencies SHOULD ensure that the default policy is to deny the execution of software.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5	
14.2.7.C.02	Application allow listing configuration	Agencies SHOULD ensure that application allow listing is used in addition to a strong access control list model and the use of limited privilege accounts.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5	
14.2.7.C.03	Application allow listing configuration	Agencies SHOULD plan and test application allow listing mechanisms and processes thoroughly prior to implementation.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5	
14.2.7.C.04	Application allow listing configuration	Agencies SHOULD restrict the decision whether to run an executable based on the following, in the order of preference shown: validates cryptographic hash; executable absolute path; digital signature; and parent folder.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5	
14.2.7.C.05	Application allow listing configuration	Agencies SHOULD restrict the process creation permissions of any executables which are permitted to run by the application allow listing controls.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5	
14.2.7.C.06	Application allow listing configuration	Agencies SHOULD validate executable behaviour, in particular process creation, permission changes and access control modifications through examination, testing, monitoring and restriction of the permissions.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5	
14.2.7.C.07	Application allow listing configuration	Logs from the application allow listing implementation SHOULD include all relevant information.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5	
14.3.5.C.01	Web usage policy	Agencies MUST develop and implement a policy governing appropriate Web usage.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
14.3.5.C.01	Web usage policy	Agencies MUST develop and implement a policy governing appropriate Web usage.	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	
14.3.6.C.01	Web proxy	Agencies SHOULD use a Web proxy for all Web browsing activities.	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
14.3.6.C.01	Web proxy	Agencies SHOULD use a Web proxy for all Web browsing activities.	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	
14.3.6.C.02	Web proxy	An agency's Web proxy SHOULD authenticate system users and provide logging that includes at least the following details about websites accessed: address (uniform resource locator); time/date; system user; internal IP address; and external IP address.	Functional	Intersects With	Proxy Logging	MON-01.9	Mechanisms exist to log all Internet-bound requests, in order to identify prohibited activities and assist incident handlers with identifying potentially compromised systems.	5	
14.3.6.C.02	Web proxy	An agency's Web proxy SHOULD authenticate system users and provide logging that includes at least the following details about websites accessed: address (uniform resource locator); time/date; system user; internal IP address; and external IP address.	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
14.3.6.C.02	Web proxy	An agency's Web proxy SHOULD authenticate system users and provide logging that includes at least the following details about websites accessed: address (uniform resource locator); time/date; system user; internal IP address; and external IP address.	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	
14.3.6.C.03	Web proxy	Agencies SHOULD NOT permit downloading of executable files from external websites unless there is a demonstrable and approved business requirement.	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
14.3.6.C.03	Web proxy	Agencies SHOULD NOT permit downloading of executable files from external websites unless there is a demonstrable and approved business requirement.	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	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
14.3.7.C.01	Applications and plug-ins	Agencies SHOULD disable the automatic launching of files downloaded from external websites.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
14.3.8.C.01	Inspection of TLS	Agencies permitting TLS through their gateways SHOULD implement: a solution that decrypts and inspects the TLS traffic as per content filtering requirements; or an allow list specifying the addresses (uniform resource locators) to which encrypted connections are permitted, with all other addresses blocked.	Functional	Intersects With	Visibility of Encrypted Communications	NET-18.2	Mechanisms exist to configure the proxy to make encrypted communications traffic visible to monitoring tools and mechanisms.	5	
14.3.9.C.01	Legal advice on the Inspection of TLS traffic	Agencies SHOULD seek legal advice regarding the inspection of encrypted TLS traffic by their gateways.	Functional	Intersects With	Visibility of Encrypted Communications	NET-18.2	Mechanisms exist to configure the proxy to make encrypted communications traffic visible to monitoring tools and mechanisms.	5	
14.3.10.C.01	Allow listing / Deny listing websites	Agencies SHOULD implement allow listing for all HTTP traffic being communicated through their gateways.	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
14.3.10.C.02	Allow listing / Deny listing websites	Agencies using an allow list on their gateways to specify the external addresses, to which encrypted connections are permitted, SHOULD specify allow list addresses by domain name or IP address.	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
14.3.10.C.03	Allow listing / Deny listing websites	If agencies do not allow list websites they SHOULD deny list websites to prevent access to known malicious websites.	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
14.3.10.C.04	Allow listing / Deny listing websites	Agencies deny listing websites SHOULD update the deny list on a frequent basis to ensure that it remains effective.	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
14.3.11.C.01	Client-side active content	Agencies SHOULD block client-side active content, such as Java and ActiveX, which are assessed as having a limited business impact.	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
14.3.11.C.02	Client-side active content	Agencies SHOULD: use client-side controls that allow JavaScript on a per website basis; and add JavaScript functions used only for malicious purposes to the agency Web content filter or IDS/IPS.	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
14.3.12.C.01	Web content filter	Agencies SHOULD use the Web proxy to filter content that is potentially harmful to system users and their workstations.	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
14.3.13.C.01	Website Passwords	Users MUST NOT use agency userID and login passwords as credentials for external websites.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
14.3.13.C.01	Website Passwords	Users MUST NOT use agency userID and login passwords as credentials for external websites.	Functional	Intersects With	Password Managers	IAC-10.11	Mechanisms exist to protect and store passwords via a password manager tool.	5	
14.3.13.C.02	Website Passwords	Users SHOULD NOT store web site authentication credentials (userID and password) on workstations, remote access devices (such as laptops) or BYO devices.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
14.3.13.C.02	Website Passwords	Users SHOULD NOT store web site authentication credentials (userID and password) on workstations, remote access devices (such as laptops) or BYO devices.	Functional	Intersects With	Password Managers	IAC-10.11	Mechanisms exist to protect and store passwords via a password manager tool.	5	
14.3.13.C.03	Website Passwords	Users SHOULD NOT use the same password for multiple websites.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
14.3.13.C.03	Website Passwords	Users SHOULD NOT use the same password for multiple websites.	Functional	Intersects With	Password Managers	IAC-10.11	Mechanisms exist to protect and store passwords via a password manager tool.	5	
14.4.4.C.01	Software development environments	Agencies SHOULD ensure that software development environments are configured such that: there are at least three separate environments covering: development; testing; and production. information flow between the environments is strictly limited according to a defined and documented change policy, with access granted only to system users with a clear business requirement; new development and modifications only take place in the development environment; and write access to the authoritative source for the software (source libraries & production environment) is disabled.	Functional	Intersects With	Secure Development Environments	TDA-07	Mechanisms exist to maintain a segmented development network to ensure a secure development environment.	5	
14.4.5.C.01	Secure programming	Agencies SHOULD ensure that software developers use secure programming practices when writing code, including: designing software to use the lowest privilege level needed to achieve its task; denying access by default; checking return values of all system calls; and validating all inputs.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5	
14.4.6.C.01	Software testing	Software SHOULD be reviewed or tested for vulnerabilities before it is used in a production environment.	Functional	Intersects With	Criticality Analysis During Development	TDA-06.1	Mechanisms exist to require the developer of the Technology Asset, Application and/or Service (TAAS) to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).	5	
14.4.6.C.01	Software testing	Software SHOULD be reviewed or tested for vulnerabilities before it is used in a production environment.	Functional	Intersects With	Threat Modeling	TDA-06.2	Mechanisms exist to perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.	5	
14.4.6.C.02	Software testing	Software SHOULD be reviewed or tested by an independent party as well as the developer.	Functional	Intersects With	Criticality Analysis During Development	TDA-06.1	Mechanisms exist to require the developer of the Technology Asset, Application and/or Service (TAAS) to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).	5	
14.4.6.C.02	Software testing	Software SHOULD be reviewed or tested by an independent party as well as the developer.	Functional	Intersects With	Threat Modeling	TDA-06.2	Mechanisms exist to perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.	5	
14.4.6.C.03	Software testing	Software development SHOULD follow secure coding practices and agency development standards.	Functional	Intersects With	Criticality Analysis During Development	TDA-06.1	Mechanisms exist to require the developer of the Technology Asset, Application and/or Service (TAAS) to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).	5	
14.4.6.C.03	Software testing	Software development SHOULD follow secure coding practices and agency development standards.	Functional	Intersects With	Threat Modeling	TDA-06.2	Mechanisms exist to perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.	5	
14.5.6.C.01	Agency website content	Agencies SHOULD review all active content on their Web servers for known information security issues.	Functional	Intersects With	Malformed Input Testing	TDA-09.4	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	
14.5.6.C.01	Agency website content	Agencies SHOULD review all active content on their Web servers for known information security issues.	Functional	Intersects With	Application Penetration Testing	TDA-09.5	Mechanisms exist to perform application-level penetration testing of custom-made Technology Assets, Applications and/or Services (TAAS).	5	
14.5.6.C.01	Agency website content	Agencies SHOULD review all active content on their Web servers for known information security issues.	Functional	Subset Of	Web Security	WEB-01	Mechanisms exist to facilitate the implementation of an enterprise-wide web management policy, as well as associated standards, controls and procedures.	10	
14.5.7.C.01	Segregation of Web application components	Agencies SHOULD minimise connectivity and access between each Web application component.	Functional	Subset Of	Web Security	WEB-01	Mechanisms exist to facilitate the implementation of an enterprise-wide web management policy, as well as associated standards, controls and procedures.	10	
14.5.7.C.01	Segregation of Web application components	Agencies SHOULD minimise connectivity and access between each Web application component.	Functional	Intersects With	Web Security Standard	WEB-07	Mechanisms exist to ensure the Open Web Application Security Project (OWASP) Application Security Verification Standard is incorporated into the organization's Secure Systems Development Lifecycle (SSDLC) process.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
14.5.7.C.01	Segregation of Web application components	Agencies SHOULD minimise connectivity and access between each Web application component.	Functional	Intersects With	Web Application Framework	WEB-08	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	5	
14.5.8.C.01	Web applications	Agencies SHOULD follow the documentation provided in the Open Web Application Security Project guide to building secure Web applications and Web services.	Functional	Subset Of	Web Security	WEB-01	Mechanisms exist to facilitate the implementation of an enterprise-wide web management policy, as well as associated standards, controls and procedures.	10	
14.5.8.C.01	Web applications	Agencies SHOULD follow the documentation provided in the Open Web Application Security Project guide to building secure Web applications and Web services.	Functional	Intersects With	Web Security Standard	WEB-07	Mechanisms exist to ensure the Open Web Application Security Project (OWASP) Application Security Verification Standard is incorporated into the organization's Secure Systems Development Lifecycle (SSDLC) process.	5	
14.5.8.C.01	Web applications	Agencies SHOULD follow the documentation provided in the Open Web Application Security Project guide to building secure Web applications and Web services.	Functional	Intersects With	Web Application Framework	WEB-08	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	5	
15.1.7.C.01	Email usage policy	Agencies MUST develop and implement a policy governing the use of email.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
15.1.7.C.01	Email usage policy	Agencies MUST develop and implement a policy governing the use of email.	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	
15.1.7.C.01	Email usage policy	Agencies MUST develop and implement a policy governing the use of email.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	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	
15.1.7.C.01	Email usage policy	Agencies MUST develop and implement a policy governing the use of email.	Functional	Intersects With	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
15.1.8.C.01	Email distribution	Agencies MUST ensure that emails containing NZEO or other nationality releasability marked information are sent only to named recipients.	Functional	Intersects With	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
15.1.8.C.02	Email distribution	Agencies MUST NOT transmit emails or other documents, containing NZEO or other nationality releasability marks, to groups or distribution lists unless the nationality of all members of the distribution lists can be confirmed.	Functional	Intersects With	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
15.1.9.C.01	Protective marking standard	Agencies SHOULD comply with the national classification system for the application of protective markings.	Functional	Intersects With	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
15.1.10.C.01	Marking tools	Agencies MUST NOT allow system users to select protective markings that the system has not been accredited to process, store or communicate.	Functional	Intersects With	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
15.1.10.C.02	Marking tools	Agencies SHOULD NOT allow a protective marking to be inserted into system user generated emails without their intervention.	Functional	Intersects With	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
15.1.10.C.03	Marking tools	Agencies SHOULD NOT permit system users replying to or forwarding an email to select a protective marking that indicates that the classification of the email is lower than a previous classification used for the email.	Functional	Intersects With	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
15.1.11.C.01	Marking classified and unclassified emails	All classified and unclassified emails MUST have a protective marking.	Functional	Intersects With	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
15.1.11.C.02	Marking classified and unclassified emails	Email protective markings MUST accurately reflect the highest classification of all elements in an email, including any attachments.	Functional	Intersects With	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
15.1.11.C.03	Marking classified and unclassified emails	Agencies SHOULD include protective markings in the email subject line or header to facilitate early identification of the classification.	Functional	Intersects With	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
15.1.12.C.01	Emails from outside the government	Where an unmarked email has originated outside the government, the agency MUST assess the information and determine how it is to be handled in accordance with the classification system.	Functional	Intersects With	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
15.1.13.C.01	Marking personal emails	Where an email is of a personal nature and does not contain government information, protective markings SHOULD NOT be used.	Functional	Intersects With	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
15.1.14.C.01	Receiving unmarked emails	Where an unmarked email has originated from a New Zealand or overseas government agency, personnel SHOULD contact the originator to determine how it is to be handled.	Functional	Intersects With	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
15.1.15.C.01	Receiving emails with unknown protective markings	Where an email is received with an unknown protective marking from a New Zealand or overseas government agency, personnel SHOULD contact the originator to determine appropriate protection measures.	Functional	Intersects With	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
15.1.16.C.01	Printing	Agencies SHOULD configure systems so that the protective markings appear at the top and bottom of every page when the email is printed, in CAPITALS and appearing as the first and last item on each page.	Functional	Intersects With	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
15.1.17.C.01	Active Web addresses within emails	Personnel SHOULD NOT send emails that contain active Web addresses or click on active Web addresses within emails they receive.	Functional	Intersects With	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
15.1.18.C.01	Awareness of email usage policies	Agencies MUST make their system users aware of the agency's email usage policies.	Functional	Intersects With	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
15.1.19.C.01	Monitoring email usage	Agencies SHOULD implement measures to monitor their personnels compliance with email usage policies.	Functional	Intersects With	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
15.1.19.C.02	Monitoring email usage	Agencies SHOULD enforce the use of approved government email systems such as SEEMAIL.	Functional	Intersects With	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
15.1.20.C.01	Public Web-based email services	Agencies SHOULD NOT allow personnel to use public Web-based email services, for processing, receiving or sending emails or attachments for official business.	Functional	Intersects With	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
15.2.36.C.01	Domain-based Message Authentication, Reporting and Conformance (DMARC)	Before implementing DMARC agencies MUST: Create a DMARC policy; List all domains, in particular those used for the sending and/or receiving of email; Review the configuration of SPF and DKIM for all active domains and all published domains; and Establish one or more monitored inboxes to receive DMARC reports.	Functional	Intersects With	Domain-Based Message Authentication Reporting and Conformance (DMARC)	NET-20.4	Mechanisms exist to implement domain signature verification protections that authenticate incoming email according to the Domain-based Message Authentication Reporting and Conformance (DMARC).	5	
15.2.36.C.02	Domain-based Message Authentication, Reporting and Conformance (DMARC)	Agencies MUST enable DMARC with a policy of p=reject for all email originating from or received by their domain(s). See 15.2.16 for a recommended approach where a domain is used for sending and/or receiving email and disruption would cause a business impact.	Functional	Intersects With	Domain-Based Message Authentication Reporting and Conformance (DMARC)	NET-20.4	Mechanisms exist to implement domain signature verification protections that authenticate incoming email according to the Domain-based Message Authentication Reporting and Conformance (DMARC).	5	
15.2.36.C.03	Domain-based Message Authentication, Reporting and Conformance (DMARC)	Agencies MUST manage "received DMARC messages" in accordance with the agency's published DMARC policy.	Functional	Intersects With	Domain-Based Message Authentication Reporting and Conformance (DMARC)	NET-20.4	Mechanisms exist to implement domain signature verification protections that authenticate incoming email according to the Domain-based Message Authentication Reporting and Conformance (DMARC).	5	
15.2.36.C.04	Domain-based Message Authentication, Reporting and Conformance (DMARC)	Agencies MUST review DMARC reports on a regular basis and address any identified anomalies or security issues.	Functional	Intersects With	Domain-Based Message Authentication Reporting and Conformance (DMARC)	NET-20.4	Mechanisms exist to implement domain signature verification protections that authenticate incoming email according to the Domain-based Message Authentication Reporting and Conformance (DMARC).	5	
15.2.36.C.05	Domain-based Message Authentication, Reporting and Conformance (DMARC)	Agencies SHOULD produce failure reports and aggregate reports according to the agency's DMARC policies.	Functional	Intersects With	Domain-Based Message Authentication Reporting and Conformance (DMARC)	NET-20.4	Mechanisms exist to implement domain signature verification protections that authenticate incoming email according to the Domain-based Message Authentication Reporting and Conformance (DMARC).	5	
15.2.37.C.01	Filtering suspicious emails and attachments	Agencies SHOULD configure the following gateway filters: inbound and outbound email, including any attachments, that contain: malicious code; content in conflict with the agency's email policy; content that cannot be identified; deny listed or unauthorised filetypes; and encrypted content, when that content cannot be inspected for malicious code or authenticated as originating from a trusted source; emails addressed to internal-use only email aliases with source addresses located from outside the domain; and all emails arriving via an external connection where the source address uses an internal agency domain name.	Functional	Intersects With	Phishing & Spam Protection	END-08	Mechanisms exist to utilize anti-phishing and spam protection technologies to detect and take action on unsolicited messages transported by electronic mail.	5	
15.2.38.C.01	Active web addresses (URL) embedded in emails	Email servers SHOULD be configured to strip active addresses and URLs and replace them with text only versions.	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	5	
15.2.39.C.01	Preventing unmarked or inappropriately marked emails	Agencies MUST prevent unmarked and inappropriately marked emails being sent to intended recipients by blocking the email at the email server, originating workstation or both.	Functional	Intersects With	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	8	
15.2.39.C.02	Preventing unmarked or inappropriately marked emails	Agencies MUST enforce protective marking of emails so that checking and filtering can take place.	Functional	Intersects With	Automated Marking	DCH-04.1	Automated mechanisms exist to mark physical media and digital files to indicate the distribution limitations, handling requirements and applicable security markings (if any) of the information to aid Data Loss Prevention (DLP) technologies.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
15.2.39.C.03	Preventing unmarked or inappropriately marked emails	Agencies SHOULD enforce protective marking of emails so that checking and filtering can take place.	Functional	Intersects With	Automated Marking	DCH-04.1	Automated mechanisms exist to mark physical media and digital files to indicate the distribution limitations, handling requirements and applicable security markings (if any) of the information to aid Data Loss Prevention (DLP) technologies.	5	
15.2.40.C.01	Blocking of outbound emails	Agencies MUST configure systems to block any outbound emails with a protective marking or endorsement indicating that the content of the email exceeds the classification of the communication path.	Functional	Intersects With	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	5	
15.2.40.C.02	Blocking of outbound emails	Agencies SHOULD configure systems to log every occurrence of a blocked email.	Functional	Intersects With	Inbound & Outbound Communications Traffic	MON-01.3	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	5	
15.2.41.C.01	Blocking of inbound emails	Agencies MUST configure email systems to reject, log and report inbound emails with protective markings indicating that the content of the email exceeds the accreditation of the receiving system.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
15.2.41.C.02	Blocking of inbound emails	Agencies SHOULD notify the intended recipient of any blocked emails.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
15.2.42.C.01	Undeliverable messages	Agencies SHOULD only send notification of undeliverable, bounced, or blocked emails to senders that can be verified via SPF or other trusted means.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
15.2.43.C.01	Automatic forwarding of emails	Agencies MUST ensure that the requirements for blocking unmarked and outbound emails are also applied to automatically forwarded emails.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
15.2.44.C.01	Open relay email servers	Agencies MUST disable open email relaying so that email servers will only relay messages destined for the agency's domain(s) and those originating from authorised systems or users within that domain.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
15.2.45.C.01	Email server maintenance activities	Agencies SHOULD perform regular email server auditing, security reviews and vulnerability analysis activities.	Functional	Intersects With	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and upgrades.	5	
15.2.46.C.01	Centralised email gateways	Where an agency has system users that send email from outside the agency's network, an authenticated and encrypted channel MUST be configured to allow email to be sent via the centralised email gateway.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
15.2.46.C.02	Centralised email gateways	Agencies SHOULD route email through a centralised 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	
15.2.46.C.03	Centralised email gateways	Where backup or alternative email gateways are in place, additional email gateways SHOULD be maintained at the same standard as the primary email gateway.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
15.2.47.C.01	Transport Layer Security (TLS)	Agencies MUST enable opportunistic TLS encryption as defined in IETFs RFC 3207 on email servers that make incoming or outgoing email connections over public infrastructure.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
15.2.47.C.02	Transport Layer Security (TLS)	Agencies SHOULD implement TLS between email servers where significant volumes of classified information are passed via email to other agencies.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
15.2.48.C.01	Mail transfer agent - strict transfer security	Agencies SHOULD enable MTA-STS to prevent the unencrypted transfer of emails between complying servers.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
15.2.48.C.02	Mail transfer agent - strict transfer security	Agencies MUST use TLS 1.2 or above when implementing MTA-STS.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
15.2.48.C.03	Mail transfer agent - strict transfer security	Agencies SHOULD enable TLS reporting when implementing MTA-STS.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
15.2.49.C.01	Sender Policy Framework (SPF)	Agencies MUST: specify mail servers using SPF or Sender ID; and mark, block or identify incoming emails that fail SPF checks for notification to the email recipient.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
15.2.49.C.02	Sender Policy Framework (SPF)	Agencies MUST: use a fail SPF record when specifying email servers; and use SPF or Sender ID to verify the authenticity of incoming emails.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
15.2.49.C.03	Sender Policy Framework (SPF)	Agencies SHOULD refer to the SPF recommendations in IETFs RFC 7208.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
15.2.50.C.01	DomainKeys Identified Mail (DKIM)	Agencies MUST enable DKIM signing on all email originating from their domain.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
15.2.50.C.02	DomainKeys Identified Mail (DKIM)	Agencies MUST use DKIM in conjunction with SPF.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
15.2.50.C.03	DomainKeys Identified Mail (DKIM)	Agencies SHOULD verify DKIM signatures on emails received, taking into account that email distribution list software typically invalidates DKIM signatures.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
15.2.50.C.04	DomainKeys Identified Mail (DKIM)	Where agencies operate email distribution list software used by external senders, agencies SHOULD configure the software so that it does not impair the validity of the senders DKIM signature.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
16.1.24.C.01	Policies and procedures	Agencies MUST: develop, implement and maintain a set of policies and procedures covering all system users: identification; authentication; authorisation; privileged access identification and management; and make their system users aware of the agency's policies and procedures.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
16.1.24.C.01	Policies and procedures	Agencies MUST: develop, implement and maintain a set of policies and procedures covering all system users: identification; authentication; authorisation; privileged access identification and management; and make their system users aware of the agency's policies and procedures.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8	
16.1.24.C.01	Policies and procedures	Agencies MUST: develop, implement and maintain a set of policies and procedures covering all system users: identification; authentication; authorisation; privileged access identification and management; and make their system users aware of the agency's policies and procedures.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	8	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
16.1.25.C.01	Implement zero trust principles	Agencies SHOULD design and implement Zero Trust principles and architecture to strengthen identification management.	Functional	Intersects With	Zero Trust Architecture (ZTA)	NET-01.1	Mechanisms exist to treat all users and devices as potential threats and prevent access to data and resources until the users can be properly authenticated and their access authorized.	8	
16.1.26.C.01	Unique system user identification	Agencies MUST ensure that all system users are: uniquely identifiable; and authorised and authenticated on each occasion that access is granted to a system.	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	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).	5	
16.1.27.C.01	Shared accounts	Agencies MUST NOT use shared credentials to access accounts.	Functional	Intersects With	Restrictions on Shared Groups / Accounts	IAC-15.5	Mechanisms exist to authorize the use of shared/group accounts only under certain organization-defined conditions.	5	
16.1.27.C.01	Shared accounts	Agencies MUST NOT use shared credentials to access accounts.	Functional	Intersects With	Credential Sharing	IAC-19	Mechanisms exist to prevent the sharing of generic IDs, passwords or other generic authentication methods.	5	
16.1.27.C.02	Shared accounts	Agencies MUST NOT use shared credentials to access administrator or privileged access accounts. NB: Break Glass accounts are exempt from this control. For further guidance on Break Glass accounts see Emergency accounts (Break Glass accounts section).	Functional	Intersects With	Restrictions on Shared Groups / Accounts	IAC-15.5	Mechanisms exist to authorize the use of shared/group accounts only under certain organization-defined conditions.	5	
16.1.27.C.02	Shared accounts	Agencies MUST NOT use shared credentials to access administrator or privileged access accounts. NB: Break Glass accounts are exempt from this control. For further guidance on Break Glass accounts see Emergency accounts (Break Glass accounts section).	Functional	Intersects With	Credential Sharing	IAC-19	Mechanisms exist to prevent the sharing of generic IDs, passwords or other generic authentication methods.	5	
16.1.27.C.03	Shared accounts	Agencies SHOULD NOT use shared credentials to access accounts.	Functional	Intersects With	Credential Sharing	IAC-19	Mechanisms exist to prevent the sharing of generic IDs, passwords or other generic authentication methods.	5	
16.1.28.C.01	System user identification for shared accounts	If agencies choose to allow shared, non user-specific accounts they MUST ensure that an independent means of determining the identification of the system user is implemented and logged.	Functional	Intersects With	Restrictions on Shared Groups / Accounts	IAC-15.5	Mechanisms exist to authorize the use of shared/group accounts only under certain organization-defined conditions.	5	
16.1.29.C.01	Methods for system user identification and authentication	Agencies MUST NOT use a numerical password (or personal identification number) as the sole method of authenticating a system user to access a system.	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	
16.1.29.C.02	Methods for system user identification and authentication	Agencies SHOULD use multi-factor authentication (MFA) when identifying and authenticating system users.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5	
16.1.30.C.01	Centralisation of Identification and Authentication Management	Agencies SHOULD assess and determine the risk of centralised access management systems, including SSO, to safely manage integration into systems and when using FIM.	Functional	Intersects With	Assessments	IAO-02	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.	8	
16.1.30.C.01	Centralisation of Identification and Authentication Management	Agencies SHOULD assess and determine the risk of centralised access management systems, including SSO, to safely manage integration into systems and when using FIM.	Functional	Intersects With	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess security, compliance and resilience risks.	5	
16.1.31.C.01	Passwords and policies	Agencies MUST ensure adequate password policies are implemented and enforced across all systems.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
16.1.31.C.02	Passwords and policies	Agencies MUST implement a password policy enforcing at least annual password changes on systems that have not implemented MFA or passwordless authentication.	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	
16.1.31.C.03	Passwords and policies	Agencies MUST implement a password policy enforcing: A minimum password length of 16 characters (e.g four words). Passwords must be long, strong and unique. This means passwords must be a minimum character length, and are a combination of unique random words, characters or numbers. NB: no explicit complexity requirements are enforced (e.g. numbers or special characters), however passwords must be unique, or random and may include special characters and numbers to achieve this.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
16.1.31.C.04	Passwords and policies	To ensure security of systems are not weakened through authentication mechanisms, at a minimum, agencies MUST: apply MFA appropriately (refer to controls in Section 16.7); ensure authentication secrets (including passwords) are securely stored; remove knowledge-based questions from authentication process (eg, dogs name, first school etc.); new passwords are screened to reduce the likelihood of previously compromised passwords; remove hints from authentication process; and change passwords when a suspected or known compromise of an account has occurred.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
16.1.31.C.05	Passwords and policies	Agencies MUST NOT: allow predictable reset passwords; store passwords in the clear on the system; and reuse passwords when resetting multiple accounts.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
16.1.31.C.06	Passwords and policies	Agencies SHOULD consider the use of location-based factors in the authentication process, (e.g., Users must be at an expected location (city, country, IP address) and provide the correct credentials for the authentication to succeed).	Functional	Intersects With	Attribute-Based Access Control (ABAC)	IAC-29	Mechanisms exist to enforce Attribute-Based Access Control (ABAC) for policy-driven, dynamic authorizations that supports the secure sharing of information.	5	
16.1.31.C.07	Passwords and policies	When creating password policies, agencies SHOULD consider implementing annual password changes.	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	
16.1.32.C.01	Protecting stored authentication information	Agencies MUST NOT allow storage of unprotected authentication information that grants system access, or decrypts an encrypted device, to be located on, or with the system or device, to which the authentication information grants access.	Functional	Intersects With	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
16.1.33.C.01	Protecting authentication data in transit	Agencies MUST ensure that system authentication data is protected when in transit on organisation networks or All-of-Government systems.	Functional	Intersects With	Group Authentication	IAC-02.1	Mechanisms exist to require individuals to be authenticated with an individual authenticator when a group authenticator is utilized.	5	
16.1.33.C.01	Protecting authentication data in transit	Agencies MUST ensure that system authentication data is protected when in transit on organisation networks or All-of-Government systems.	Functional	Intersects With	Restrictions on Shared Groups / Accounts	IAC-15.5	Mechanisms exist to authorize the use of shared/group accounts only under certain organization-defined conditions.	5	
16.1.34.C.01	Hashing	Password and other authentication secrets MUST be hashed before storage using an approved cryptographic protocol and algorithm. See Chapter 17 - Cryptography.	Functional	Intersects With	Group Authentication	IAC-02.1	Mechanisms exist to require individuals to be authenticated with an individual authenticator when a group authenticator is utilized.	5	
16.1.34.C.01	Hashing	Password and other authentication secrets MUST be hashed before storage using an approved cryptographic protocol and algorithm. See Chapter 17 - Cryptography.	Functional	Intersects With	Restrictions on Shared Groups / Accounts	IAC-15.5	Mechanisms exist to authorize the use of shared/group accounts only under certain organization-defined conditions.	5	
16.1.34.C.02	Hashing	Passwords and other authentication secrets MUST be stored securely including being: salted (32 bits or more), salts should be unique to each password and should be randomly generated. hashed (HMAC using SHA-2/3), and "stretched"[such as PBKDF2 with at least: 600k iterations with internal hash function of HMAC-SHA-256; or 210k iterations with internal hash function of HMAC-SHA-512).	Functional	Intersects With	Protection of Authenticators	IAC-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	5	
16.1.35.C.01	Identification of foreign nationals	Where systems contain NZEO or other nationalities releasability marked or protectively marked information, agencies MUST provide a mechanism that allows system users and processes to identify users who are foreign nationals, including seconded foreign nationals.	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	
16.1.35.C.02	Identification of foreign nationals	Agencies using NZEO systems SHOULD ensure that identification includes specific nationality for all foreign nationals, including seconded foreign nationals.	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	
16.1.36.C.01	Resetting passwords and authentication vectors	Agencies MUST ensure system users provide sufficient evidence to prove they are the owner of the account when requesting a password reset for their system account or making changes to their multi-factor authenticators.	Functional	Intersects With	Protection of Authenticators	IAC-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
16.1.36.C.01	Resetting passwords and authentication vectors	Agencies MUST ensure system users provide sufficient evidence to prove they are the owner of the account when requesting a password reset for their system account or making changes to their multi-factor authenticators.	Functional	Intersects With	No Embedded Unencrypted Static Authenticators	IAC-10.6	Mechanisms exist to ensure that unencrypted, static authenticators are not embedded in applications, scripts or stored on function keys.	5	
16.1.36.C.02	Resetting passwords and authentication vectors	Where passwords are not set by the account holder, agencies MUST use temporary passwords when resetting system user accounts.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
16.1.36.C.03	Resetting passwords and authentication vectors	Agencies SHOULD NOT use single factor authentication when changing users Multi-Factor Authentication details.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
16.1.37.C.01	Securing Passwords	Password managers provide no additional security to the sign-in password. Agencies using password managers MUST ensure sign-in passwords adhere to the password security policies used by the organisation.	Functional	Intersects With	Protection of Authenticators	IAC-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	5	
16.1.37.C.02	Securing Passwords	Agencies using password managers SHOULD consider the use of MFA to access the password manager.	Functional	Intersects With	Password Managers	IAC-10.11	Mechanisms exist to protect and store passwords via a password manager tool.	5	
16.1.38.C.01	Passwordless Authentication	When moving to passwordless authentication, agencies SHOULD carry out a risk assessment and evaluate passwordless authentication models to choose authentication mechanisms and factors that best fit the organisations security and authentication requirements.	Functional	Intersects With	Protection of Authenticators	IAC-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	5	
16.1.39.C.01	Disabling vulnerable authentication mechanisms	Agencies MUST ensure authentication methods that are susceptible to replay attacks are disabled.	Functional	Intersects With	Citizenship Identification	HRS-04.4	Mechanisms exist to identify foreign nationals, including by their specific citizenship.	5	
16.1.39.C.02	Disabling vulnerable authentication mechanisms	Agencies MUST disable LAN Manager for password authentication on workstations and servers.	Functional	Intersects With	Citizenship Identification	HRS-04.4	Mechanisms exist to identify foreign nationals, including by their specific citizenship.	5	
16.1.40.C.01	Session termination	Agencies SHOULD develop and implement a policy to automatically logout and shutdown workstations after an appropriate time of inactivity. This includes invalidating any session tokens.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
16.1.41.C.01	Screen and session locking	Agencies MUST: configure systems with a screen and session lock; configure the lock to activate: after a maximum of 10 minutes of system user inactivity; or if manually activated by the system user; configure the lock to completely conceal all information on the screen; ensure that the screen is not turned off or enters a power saving state before the screen or session lock is activated; have the user reauthenticate to unlock the system; and deny users the ability to disable the locking mechanism.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
16.1.41.C.01	Screen and session locking	Agencies MUST: configure systems with a screen and session lock; configure the lock to activate: after a maximum of 10 minutes of system user inactivity; or if manually activated by the system user; configure the lock to completely conceal all information on the screen; ensure that the screen is not turned off or enters a power saving state before the screen or session lock is activated; have the user reauthenticate to unlock the system; and deny users the ability to disable the locking mechanism.	Functional	Intersects With	Automated Support For Password Strength	IAC-10.4	Automated mechanisms exist to determine if password authenticators are sufficiently strong enough to satisfy organization-defined password length and complexity requirements.	5	
16.1.41.C.02	Screen and session locking	Agencies SHOULD: configure systems with a session or screen lock; configure the lock to activate: after a maximum of 10 minutes of system user inactivity; or if manually activated by the system user; configure the lock to completely conceal all information on the screen; ensure that the screen is not turned off or enters a power saving state before the screen or session lock is activated; have the system user reauthenticate to unlock the system; and deny system users the ability to disable the locking mechanism.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
16.1.41.C.02	Screen and session locking	Agencies SHOULD: configure systems with a session or screen lock; configure the lock to activate: after a maximum of 10 minutes of system user inactivity; or if manually activated by the system user; configure the lock to completely conceal all information on the screen; ensure that the screen is not turned off or enters a power saving state before the screen or session lock is activated; have the system user reauthenticate to unlock the system; and deny system users the ability to disable the locking mechanism.	Functional	Intersects With	Automated Support For Password Strength	IAC-10.4	Automated mechanisms exist to determine if password authenticators are sufficiently strong enough to satisfy organization-defined password length and complexity requirements.	5	
16.1.42.C.01	Suspension of access	Agencies MUST: Record all successful and failed logon attempts; lock system user accounts after three failed logon attempts; use a temporary lock out feature to unlock system (max [] times); have a system administrator reset locked accounts if [] times is superseded; remove or suspend system user accounts as soon as possible when personnel no longer need access due to changing roles or leaving the organisation; and remove or suspend inactive accounts after a specified number of days. NB: Agencies can determine the risk of using a temporary lock out feature on their specific systems. [] indicates the chosen 'value of times' an agency has decided to use for the temporary lock out feature.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
16.1.42.C.01	Suspension of access	Agencies MUST: Record all successful and failed logon attempts; lock system user accounts after three failed logon attempts; use a temporary lock out feature to unlock system (max [] times); have a system administrator reset locked accounts if [] times is superseded; remove or suspend system user accounts as soon as possible when personnel no longer need access due to changing roles or leaving the organisation; and remove or suspend inactive accounts after a specified number of days. NB: Agencies can determine the risk of using a temporary lock out feature on their specific systems. [] indicates the chosen 'value of times' an agency has decided to use for the temporary lock out feature.	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	
16.1.43.C.01	Investigating repeated account lockouts	Agencies SHOULD ensure that repeated account lockouts are investigated before reauthorising access.	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	
16.1.44.C.01	Logon banner	Agencies SHOULD have a logon banner that requires a system user to acknowledge and accept their security responsibilities before access to the system is granted.	Functional	Intersects With	Session Termination	IAC-25	Automated mechanisms exist to log out users, both locally on the network and for remote sessions, at the end of the session or after an organization-defined period of inactivity.	5	
16.1.44.C.02	Logon banner	Agencies SHOULD seek legal advice on the exact wording of logon banners.	Functional	Intersects With	System Use Notification (Logon Banner)	SEA-18	Mechanisms exist to utilize system use notification / logon banners that display an approved system use notification message or banner before granting access to Technology Assets, Applications and/or Services (TAAS).	5	
16.1.44.C.03	Logon banner	Agency logon banners SHOULD cover issues such as: the systems classification; access only being permitted to authorised system users; the system users agreement to abide by relevant security policies; the system users awareness of the possibility that system usage is being monitored; the definition of acceptable use for the system; and legal ramifications of violating the relevant policies.	Functional	Intersects With	System Use Notification (Logon Banner)	SEA-18	Mechanisms exist to utilize system use notification / logon banners that display an approved system use notification message or banner before granting access to Technology Assets, Applications and/or Services (TAAS).	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
16.2.4.C.01	Access control lists	Agencies MUST follow a defined process for developing an access control list, such as described in the table below. Stage Description 1 Establish groups of all system resources based on similar security objectives. 2 Determine the information owner for each group of resources. 3 Obtain agreement from system owners. 4 Establish groups encompassing all system users based on similar functions or security objectives. 5 Determine the group owner or manager for each group of system users. 6 Determine the degree of access to the resource for each system user group, incorporating the principal of least-privilege access. 7 Decide on the level of access for security administration, based on the internal security policy. 8 Identify any classification, protective markings, and releasability indicators (such as NZEO or compartmented information)	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5	
16.2.4.C.01	Access control lists	Agencies MUST follow a defined process for developing an access control list, such as described in the table below. Stage Description 1 Establish groups of all system resources based on similar security objectives. 2 Determine the information owner for each group of resources. 3 Obtain agreement from system owners. 4 Establish groups encompassing all system users based on similar functions or security objectives. 5 Determine the group owner or manager for each group of system users. 6 Determine the degree of access to the resource for each system user group, incorporating the principal of least-privilege access. 7 Decide on the level of access for security administration, based on the internal security policy. 8 Identify any classification, protective markings, and releasability indicators (such as NZEO or compartmented information)	Functional	Intersects With	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
16.2.5.C.01	Enforcing authorisations on systems	Agencies MUST have authorisation of system users enforced by access controls.	Functional	Intersects With	Data Access Mapping	DCH-14.3	Mechanisms exist to leverage data-specific Access Control Lists (ACL) or Interconnection Security Agreements (ISAs) to generate a logical map of the parties with whom sensitive and/or regulated data is shared.	5	
16.2.5.C.01	Enforcing authorisations on systems	Agencies MUST have authorisation of system users enforced by access controls.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5	
16.2.6.C.01	Protecting compartmented information on systems	Agencies MUST restrict access to compartmented information. Such restriction MUST be enforced by the system.	Functional	Intersects With	Data Access Mapping	DCH-14.3	Mechanisms exist to leverage data-specific Access Control Lists (ACL) or Interconnection Security Agreements (ISAs) to generate a logical map of the parties with whom sensitive and/or regulated data is shared.	5	
16.2.7.C.01	Access from foreign controlled systems and facilities	Agencies MUST NOT allow access to NZEO information from systems and facilities not under the sole control of the government of New Zealand and New Zealand citizens.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive and/or regulated data wherever it is processed and/or stored.	5	
16.2.7.C.02	Access from foreign controlled systems and facilities	Unless a multilateral or bilateral security agreement is in place, agencies SHOULD NOT allow access to classified information from systems and facilities not under the sole control of the government of New Zealand and New Zealand citizens.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive and/or regulated data wherever it is processed and/or stored.	5	
16.3.5.C.01	Use of privileged accounts	Agencies MUST: ensure strong change management practices are implemented; ensure that the use of privileged accounts is controlled and accountable; ensure that system administrators are assigned, and consistently use, an individual account for the performance of their administration tasks; keep privileged accounts to a minimum; and allow the use of privileged accounts for administrative work only.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5	
16.3.6.C.01	Privileged system access by foreign nationals	Agencies MUST NOT allow foreign nationals, including seconded foreign nationals, to have privileged access to systems that process, store or communicate NZEO information.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5	
16.3.6.C.02	Privileged system access by foreign nationals	Agencies SHOULD NOT allow foreign nationals, including seconded foreign nationals, to have privileged access to systems that process, store or communicate classified information.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5	
16.3.7.C.01	Security clearances for privileged users	Agencies involved in frequent transfers of data from another system to their system with a lesser classification SHOULD ensure at least one privileged user has a security clearance level commensurate the classification of the higher system.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5	
16.4.36.C.01	Policy Creation and Implementation	Agencies MUST establish a Privileged Access Management (PAM) policy.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5	
16.4.36.C.02	Policy Creation and Implementation	Within the context of agency operations, the agency's PAM policy MUST define: a privileged account; and privileged access.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5	
16.4.36.C.03	Policy Creation and Implementation	Agencies MUST manage privileged accounts in accordance with the agency's PAM policy.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5	
16.4.37.C.01	The Principle of Least Privilege	Agencies MUST apply the Principle of Least Privilege when developing and implementing a Privileged Access Management (PAM) policy.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5	
16.4.37.C.01	The Principle of Least Privilege	Agencies MUST apply the Principle of Least Privilege when developing and implementing a Privileged Access Management (PAM) policy.	Functional	Intersects With	User Responsibilities for Account Management	IAC-18	Mechanisms exist to compel users to follow accepted practices in the use of authentication mechanisms (e.g., passwords, passphrases, physical or logical security tokens, smart cards, certificates, etc.).	5	
16.4.37.C.02	The Principle of Least Privilege	Agencies MUST use two-factor or Multi-Factor Authentication to allow access to privileged accounts.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5	
16.4.37.C.03	The Principle of Least Privilege	Agencies SHOULD consider the use of time bound revocation to privileged accounts.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5	
16.4.38.C.01	Strong Authentication process	As part of a Privileged Access Management (PAM) policy, agencies MUST establish and implement a strong approval and authorisation process before any privileged access credentials are issued.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5	
16.4.38.C.02	Strong Authentication process	Privileged Access credentials MUST NOT be issued until approval has been formally granted.	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	
16.4.38.C.02	Strong Authentication process	Privileged Access credentials MUST NOT be issued until approval has been formally granted.	Functional	Intersects With	User Responsibilities for Account Management	IAC-18	Mechanisms exist to compel users to follow accepted practices in the use of authentication mechanisms (e.g., passwords, passphrases, physical or logical security tokens, smart cards, certificates, etc.).	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
16.4.39.C.01	Suspension and Revocation of Privileged Access Credentials	Agencies MUST establish robust credential suspension and revocation procedures as part of the agency's Privileged Access Management (PAM) policy.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
16.4.39.C.02	Suspension and Revocation of Privileged Access Credentials	Agencies MUST investigate any indication of compromise or misuse of systems credentials or accounts.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
16.4.40.C.01	Privileged Account, Rights and Credential Inventory	Agencies MUST create and maintain a comprehensive inventory of privileged accounts and the associated access rights and credentials.	Functional	Intersects With	Privileged Account Inventories	IAC-16.1	Mechanisms exist to inventory all privileged accounts and validate that each person with elevated privileges is authorized by the appropriate level of organizational management.	5	
16.4.41.C.01	Monitoring and Review	Agencies MUST create, implement and maintain a robust system of continuous discovery, monitoring and review of privileged accounts and the access rights and credentials associated with those accounts.	Functional	Intersects With	Privileged Functions Logging	MON-03.3	Mechanisms exist to log and review the actions of users and/or services with elevated privileges.	5	
16.4.41.C.02	Monitoring and Review	Privileged account monitoring systems MUST monitor and record: individual user activity, including exceptions such as out of hours access; activity from unauthorised sources; any unusual use patterns; and any creation of unauthorised privileges access credentials.	Functional	Intersects With	Privileged Functions Logging	MON-03.3	Mechanisms exist to log and review the actions of users and/or services with elevated privileges.	5	
16.4.41.C.03	Monitoring and Review	Agencies MUST protect and limit access to activity and audit logs and records.	Functional	Intersects With	Access by Subset of Privileged Users	MON-08.2	Mechanisms exist to restrict access to the management of event logs to privileged users with a specific business need.	5	
16.4.42.C.01	Response and Remediation	Agencies MUST develop and implement a response and remediation policy and procedure as part of an agency's Privileged Access Management (PAM) policy.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
16.4.43.C.01	User Education and Awareness	Agencies MUST implement a Privileged Access Management (PAM) policy training module as part of the agency's overall user training and awareness requirement.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	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	
16.5.10.C.01	Authentication	Agencies MUST authenticate each remote connection and user prior to permitting access to an agency system.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	
16.5.10.C.02	Authentication	Agencies SHOULD authenticate both the remote system user and device during the authentication process.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	
16.5.11.C.01	Remote privileged access	Agencies MUST NOT allow the use of remote privileged access from an untrusted domain, including logging in as an unprivileged system user and then escalating privileges.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	
16.5.11.C.01	Remote privileged access	Agencies MUST NOT allow the use of remote privileged access from an untrusted domain, including logging in as an unprivileged system user and then escalating privileges.	Functional	Intersects With	Remote Privileged Commands & Sensitive Data Access	NET-14.4	Mechanisms exist to restrict the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs.	5	
16.5.11.C.02	Remote privileged access	Agencies SHOULD NOT allow the use of remote privileged access from an untrusted domain, including logging in as an unprivileged system user and then escalating privileges.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	
16.5.11.C.02	Remote privileged access	Agencies SHOULD NOT allow the use of remote privileged access from an untrusted domain, including logging in as an unprivileged system user and then escalating privileges.	Functional	Intersects With	Remote Privileged Commands & Sensitive Data Access	NET-14.4	Mechanisms exist to restrict the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs.	5	
16.5.12.C.01	Virtual Private Networks (VPNs)	Agencies SHOULD establish VPN connections for all remote access connections.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	
16.5.12.C.02	Virtual Private Networks (VPNs)	Agencies SHOULD use Zero Trust principles alongside the use of VPN connections to enhance the security posture of the organisation. This should include removing the ability for a standard user to disable the VPN connection.	Functional	Intersects With	Zero Trust Architecture (ZTA)	NET-01.1	Mechanisms exist to treat all users and devices as potential threats and prevent access to data and resources until the users can be properly authenticated and their access authorized.	5	
16.6.6.C.01	Maintaining system management logs	Agencies MUST maintain system management logs for the life of a system.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
16.6.6.C.01	Maintaining system management logs	Agencies MUST maintain system management logs for the life of a system.	Functional	Intersects With	Analyze and Prioritize Monitoring Requirements	MON-01.16	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	
16.6.6.C.02	Maintaining system management logs	Agencies SHOULD determine a policy for the retention of system management logs.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
16.6.6.C.02	Maintaining system management logs	Agencies SHOULD determine a policy for the retention of system management logs.	Functional	Intersects With	Analyze and Prioritize Monitoring Requirements	MON-01.16	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	
16.6.7.C.01	Content of system management logs	A system management log SHOULD record the following minimum information: all system start-up and shutdown; all system changes; user changes; service, application, component or system failures; maintenance activities; backup and archival activities; system recovery activities; and special or out of hours activities.	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5	
16.6.7.C.01	Content of system management logs	A system management log SHOULD record the following minimum information: all system start-up and shutdown; all system changes; user changes; service, application, component or system failures; maintenance activities; backup and archival activities; system recovery activities; and special or out of hours activities.	Functional	Intersects With	Database Logging	MON-03.7	Mechanisms exist to ensure databases produce audit records that contain sufficient information to monitor database activities.	5	
16.6.8.C.01	Logging requirements	Agencies MUST develop and document logging requirements covering: the logging facility, including: log server availability requirements; and the reliable delivery of log information to the log server; the list of events associated with a system or software component to be logged; and event log protection and archival requirements.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
16.6.8.C.01	Logging requirements	Agencies MUST develop and document logging requirements covering: the logging facility, including: log server availability requirements; and the reliable delivery of log information to the log server; the list of events associated with a system or software component to be logged; and event log protection and archival requirements.	Functional	Intersects With	Analyze and Prioritize Monitoring Requirements	MON-01.16	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	
16.6.8.C.01	Logging requirements	Agencies MUST develop and document logging requirements covering: the logging facility, including: log server availability requirements; and the reliable delivery of log information to the log server; the list of events associated with a system or software component to be logged; and event log protection and archival requirements.	Functional	Intersects With	Audit Trails	MON-03.2	Mechanisms exist to link system access to individual users or service accounts.	5	
16.6.9.C.01	Events to be logged	Agencies MUST log, at minimum, the following events for all software components: any login activity or attempts; date and time; all privileged operations; failed attempts to elevate privileges; security related system alerts and failures; software upgrades and/or software patching; system recovery activities; system user and group additions, deletions and modification to permissions; and unauthorised or failed access attempts to systems and files identified as critical to the organisation.	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5	

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
16.6.9.C.01	Events to be logged	Agencies MUST log, at minimum, the following events for all software components: any login activity or attempts; date and time; all privileged operations; failed attempts to elevate privileges; security related system alerts and failures; software upgrades and/or software patching; system recovery activities; system user and group additions, deletions and modification to permissions; and unauthorised or failed access attempts to systems and files identified as critical to the organisation.	Functional	Intersects With	Audit Trails	MON-03.2	Mechanisms exist to link system access to individual users or service accounts.	5	
16.6.9.C.01	Events to be logged	Agencies MUST log, at minimum, the following events for all software components: any login activity or attempts; date and time; all privileged operations; failed attempts to elevate privileges; security related system alerts and failures; software upgrades and/or software patching; system recovery activities; system user and group additions, deletions and modification to permissions; and unauthorised or failed access attempts to systems and files identified as critical to the organisation.	Functional	Intersects With	Database Logging	MON-03.7	Mechanisms exist to ensure databases produce audit records that contain sufficient information to monitor database activities.	5	
16.6.10.C.01	Additional events to be logged	Agencies SHOULD log the events listed in the table below for specific software components. Software component Events to log Database System user access to the database. Attempted access that is denied. Changes to system user roles or database rights. Addition of new system users, especially privileged users. Modifications to the data. Modifications to the format or structure of the database. Network/operating system Successful and failed attempts to logon and logoff. Changes to system administrator and system user accounts. Failed attempts to access data and system resources. Attempts to use special privileges. Use of special privileges. System user or group management. Changes to the security policy. Service failures and restarts. System startup and shutdown. Changes to system configuration data. Access to sensitive data and processes. Data import/export operations. Web application System user access to the Web application. Attempted access that is denied. System user access to the Web documents. Search engine queries initiated by system users	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
16.6.10.C.01	Additional events to be logged	Agencies SHOULD log the events listed in the table below for specific software components. Software component Events to log Database System user access to the database. Attempted access that is denied. Changes to system user roles or database rights. Addition of new system users, especially privileged users. Modifications to the data. Modifications to the format or structure of the database. Network/operating system Successful and failed attempts to logon and logoff. Changes to system administrator and system user accounts. Failed attempts to access data and system resources. Attempts to use special privileges. Use of special privileges. System user or group management. Changes to the security policy. Service failures and restarts. System startup and shutdown. Changes to system configuration data. Access to sensitive data and processes. Data import/export operations. Web application System user access to the Web application. Attempted access that is denied. System user access to the Web documents. Search engine queries initiated by system users	Functional	Intersects With	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	5	
16.6.10.C.01	Additional events to be logged	Agencies SHOULD log the events listed in the table below for specific software components. Software component Events to log Database System user access to the database. Attempted access that is denied. Changes to system user roles or database rights. Addition of new system users, especially privileged users. Modifications to the data. Modifications to the format or structure of the database. Network/operating system Successful and failed attempts to logon and logoff. Changes to system administrator and system user accounts. Failed attempts to access data and system resources. Attempts to use special privileges. Use of special privileges. System user or group management. Changes to the security policy. Service failures and restarts. System startup and shutdown. Changes to system configuration data. Access to sensitive data and processes. Data import/export operations. Web application System user access to the Web application. Attempted access that is denied. System user access to the Web documents. Search engine queries initiated by system users	Functional	Intersects With	Inbound & Outbound Communications Traffic	MON-01.3	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	5	

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
16.6.10.C.01	Additional events to be logged	Agencies SHOULD log the events listed in the table below for specific software components. Software component Events to log Database System user access to the database. Attempted access that is denied. Changes to system user roles or database rights. Addition of new system users, especially privileged users. Modifications to the data. Modifications to the format or structure of the database. Network/operating system Successful and failed attempts to logon and logoff. Changes to system administrator and system user accounts. Failed attempts to access data and system resources. Attempts to use special privileges. Use of special privileges. System user or group management. Changes to the security policy. Service failures and restarts. System startup and shutdown. Changes to system configuration data. Access to sensitive data and processes. Data import/export operations. Web application System user access to the Web application. Attempted access that is denied. System user access to the Web documents. Search engine queries initiated by system users	Functional	Intersects With	Wireless Network Monitoring	MON-01.5	Mechanisms exist to monitor wireless network segments for: (1) Rogue wireless devices; and (2) Anomalous and/or hostile activities.	5	
16.6.10.C.01	Additional events to be logged	Agencies SHOULD log the events listed in the table below for specific software components. Software component Events to log Database System user access to the database. Attempted access that is denied. Changes to system user roles or database rights. Addition of new system users, especially privileged users. Modifications to the data. Modifications to the format or structure of the database. Network/operating system Successful and failed attempts to logon and logoff. Changes to system administrator and system user accounts. Failed attempts to access data and system resources. Attempts to use special privileges. Use of special privileges. System user or group management. Changes to the security policy. Service failures and restarts. System startup and shutdown. Changes to system configuration data. Access to sensitive data and processes. Data import/export operations. Web application System user access to the Web application. Attempted access that is denied. System user access to the Web documents. Search engine queries initiated by system users	Functional	Intersects With	File Integrity Monitoring (FIM)	MON-01.7	Mechanisms exist to utilize a File Integrity Monitor (FIM), or similar change-detection technology, on critical Technology Assets, Applications and/or Services (TAAS) to generate alerts for unauthorized modifications.	5	
16.6.10.C.01	Additional events to be logged	Agencies SHOULD log the events listed in the table below for specific software components. Software component Events to log Database System user access to the database. Attempted access that is denied. Changes to system user roles or database rights. Addition of new system users, especially privileged users. Modifications to the data. Modifications to the format or structure of the database. Network/operating system Successful and failed attempts to logon and logoff. Changes to system administrator and system user accounts. Failed attempts to access data and system resources. Attempts to use special privileges. Use of special privileges. System user or group management. Changes to the security policy. Service failures and restarts. System startup and shutdown. Changes to system configuration data. Access to sensitive data and processes. Data import/export operations. Web application System user access to the Web application. Attempted access that is denied. System user access to the Web documents. Search engine queries initiated by system users	Functional	Intersects With	Proxy Logging	MON-01.9	Mechanisms exist to log all Internet-bound requests, in order to identify prohibited activities and assist incident handlers with identifying potentially compromised systems.	5	
16.6.10.C.01	Additional events to be logged	Agencies SHOULD log the events listed in the table below for specific software components. Software component Events to log Database System user access to the database. Attempted access that is denied. Changes to system user roles or database rights. Addition of new system users, especially privileged users. Modifications to the data. Modifications to the format or structure of the database. Network/operating system Successful and failed attempts to logon and logoff. Changes to system administrator and system user accounts. Failed attempts to access data and system resources. Attempts to use special privileges. Use of special privileges. System user or group management. Changes to the security policy. Service failures and restarts. System startup and shutdown. Changes to system configuration data. Access to sensitive data and processes. Data import/export operations. Web application System user access to the Web application. Attempted access that is denied. System user access to the Web documents. Search engine queries initiated by system users	Functional	Intersects With	Analyze and Prioritize Monitoring Requirements	MON-01.16	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	

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
16.6.10.C.01	Additional events to be logged	Agencies SHOULD log the events listed in the table below for specific software components. Software component Events to log Database System user access to the database. Attempted access that is denied. Changes to system user roles or database rights. Addition of new system users, especially privileged users. Modifications to the data. Modifications to the format or structure of the database. Network/operating system Successful and failed attempts to logon and logoff. Changes to system administrator and system user accounts. Failed attempts to access data and system resources. Attempts to use special privileges. Use of special privileges. System user or group management. Changes to the security policy. Service failures and restarts. System startup and shutdown. Changes to system configuration data. Access to sensitive data and processes. Data import/export operations. Web application System user access to the Web application. Attempted access that is denied. System user access to the Web documents. Search engine queries initiated by system users	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5	
16.6.10.C.01	Additional events to be logged	Agencies SHOULD log the events listed in the table below for specific software components. Software component Events to log Database System user access to the database. Attempted access that is denied. Changes to system user roles or database rights. Addition of new system users, especially privileged users. Modifications to the data. Modifications to the format or structure of the database. Network/operating system Successful and failed attempts to logon and logoff. Changes to system administrator and system user accounts. Failed attempts to access data and system resources. Attempts to use special privileges. Use of special privileges. System user or group management. Changes to the security policy. Service failures and restarts. System startup and shutdown. Changes to system configuration data. Access to sensitive data and processes. Data import/export operations. Web application System user access to the Web application. Attempted access that is denied. System user access to the Web documents. Search engine queries initiated by system users	Functional	Intersects With	Audit Trails	MON-03.2	Mechanisms exist to link system access to individual users or service accounts.	5	
16.6.10.C.01	Additional events to be logged	Agencies SHOULD log the events listed in the table below for specific software components. Software component Events to log Database System user access to the database. Attempted access that is denied. Changes to system user roles or database rights. Addition of new system users, especially privileged users. Modifications to the data. Modifications to the format or structure of the database. Network/operating system Successful and failed attempts to logon and logoff. Changes to system administrator and system user accounts. Failed attempts to access data and system resources. Attempts to use special privileges. Use of special privileges. System user or group management. Changes to the security policy. Service failures and restarts. System startup and shutdown. Changes to system configuration data. Access to sensitive data and processes. Data import/export operations. Web application System user access to the Web application. Attempted access that is denied. System user access to the Web documents. Search engine queries initiated by system users	Functional	Intersects With	Database Logging	MON-03.7	Mechanisms exist to ensure databases produce audit records that contain sufficient information to monitor database activities.	5	
16.6.10.C.02	Additional events to be logged	Agencies SHOULD log, at minimum, the following events for all software components: Any login activity or attempts; all privileged operations; failed attempts to elevate privileges; security related system alerts and failures; all software updates and/or patching; system user and group additions, deletions and modification to permissions; and unauthorised or failed access attempts to systems and files identified as critical to the organisation.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
16.6.10.C.02	Additional events to be logged	Agencies SHOULD log, at minimum, the following events for all software components: Any login activity or attempts; all privileged operations; failed attempts to elevate privileges; security related system alerts and failures; all software updates and/or patching; system user and group additions, deletions and modification to permissions; and unauthorised or failed access attempts to systems and files identified as critical to the organisation.	Functional	Intersects With	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	5	
16.6.10.C.02	Additional events to be logged	Agencies SHOULD log, at minimum, the following events for all software components: Any login activity or attempts; all privileged operations; failed attempts to elevate privileges; security related system alerts and failures; all software updates and/or patching; system user and group additions, deletions and modification to permissions; and unauthorised or failed access attempts to systems and files identified as critical to the organisation.	Functional	Intersects With	Inbound & Outbound Communications Traffic	MON-01.3	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
16.6.10.C.02	Additional events to be logged	Agencies SHOULD log, at minimum, the following events for all software components: Any login activity or attempts; all privileged operations; failed attempts to elevate privileges; security related system alerts and failures; all software updates and/or patching; system user and group additions, deletions and modification to permissions; and unauthorised or failed access attempts to systems and files identified as critical to the organisation.	Functional	Intersects With	Wireless Network Monitoring	MON-01.5	Mechanisms exist to monitor wireless network segments for: (1) Rogue wireless devices; and (2) Anomalous and/or hostile activities.	5	
16.6.10.C.02	Additional events to be logged	Agencies SHOULD log, at minimum, the following events for all software components: Any login activity or attempts; all privileged operations; failed attempts to elevate privileges; security related system alerts and failures; all software updates and/or patching; system user and group additions, deletions and modification to permissions; and unauthorised or failed access attempts to systems and files identified as critical to the organisation.	Functional	Intersects With	File Integrity Monitoring (FIM)	MON-01.7	Mechanisms exist to utilize a File Integrity Monitor (FIM), or similar change-detection technology, on critical Technology Assets, Applications and/or Services (TAAS) to generate alerts for unauthorized modifications.	5	
16.6.10.C.02	Additional events to be logged	Agencies SHOULD log, at minimum, the following events for all software components: Any login activity or attempts; all privileged operations; failed attempts to elevate privileges; security related system alerts and failures; all software updates and/or patching; system user and group additions, deletions and modification to permissions; and unauthorised or failed access attempts to systems and files identified as critical to the organisation.	Functional	Intersects With	Proxy Logging	MON-01.9	Mechanisms exist to log all Internet-bound requests, in order to identify prohibited activities and assist incident handlers with identifying potentially compromised systems.	5	
16.6.10.C.02	Additional events to be logged	Agencies SHOULD log, at minimum, the following events for all software components: Any login activity or attempts; all privileged operations; failed attempts to elevate privileges; security related system alerts and failures; all software updates and/or patching; system user and group additions, deletions and modification to permissions; and unauthorised or failed access attempts to systems and files identified as critical to the organisation.	Functional	Intersects With	Analyze and Prioritize Monitoring Requirements	MON-01.16	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	
16.6.10.C.02	Additional events to be logged	Agencies SHOULD log, at minimum, the following events for all software components: Any login activity or attempts; all privileged operations; failed attempts to elevate privileges; security related system alerts and failures; all software updates and/or patching; system user and group additions, deletions and modification to permissions; and unauthorised or failed access attempts to systems and files identified as critical to the organisation.	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5	
16.6.10.C.02	Additional events to be logged	Agencies SHOULD log, at minimum, the following events for all software components: Any login activity or attempts; all privileged operations; failed attempts to elevate privileges; security related system alerts and failures; all software updates and/or patching; system user and group additions, deletions and modification to permissions; and unauthorised or failed access attempts to systems and files identified as critical to the organisation.	Functional	Intersects With	Audit Trails	MON-03.2	Mechanisms exist to link system access to individual users or service accounts.	5	
16.6.10.C.02	Additional events to be logged	Agencies SHOULD log, at minimum, the following events for all software components: Any login activity or attempts; all privileged operations; failed attempts to elevate privileges; security related system alerts and failures; all software updates and/or patching; system user and group additions, deletions and modification to permissions; and unauthorised or failed access attempts to systems and files identified as critical to the organisation.	Functional	Intersects With	Database Logging	MON-03.7	Mechanisms exist to ensure databases produce audit records that contain sufficient information to monitor database activities.	5	
16.6.11.C.01	Event log facility	For each event identified as needing to be logged, agencies MUST ensure that the log facility records at least the following details, where applicable: date and time of the event; relevant system user(s) or processes; event description; success or failure of the event; event source (e.g. application name); and IT equipment location/identification.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	
16.6.11.C.01	Event log facility	For each event identified as needing to be logged, agencies MUST ensure that the log facility records at least the following details, where applicable: date and time of the event; relevant system user(s) or processes; event description; success or failure of the event; event source (e.g. application name); and IT equipment location/identification.	Functional	Intersects With	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.	5	
16.6.11.C.02	Event log facility	Agencies SHOULD establish an authoritative time source.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	
16.6.11.C.02	Event log facility	Agencies SHOULD establish an authoritative time source.	Functional	Intersects With	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.	5	
16.6.11.C.02	Event log facility	Agencies SHOULD establish an authoritative time source.	Functional	Intersects With	System-Wide / Time-Correlated Audit Trail	MON-02.7	Automated mechanisms exist to compile audit records into an organization-wide audit trail that is time-correlated.	5	
16.6.11.C.03	Event log facility	Agencies SHOULD synchronise all logging and audit trails with the time source to allow accurate time stamping of events.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	
16.6.11.C.03	Event log facility	Agencies SHOULD synchronise all logging and audit trails with the time source to allow accurate time stamping of events.	Functional	Intersects With	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.	5	
16.6.12.C.01	Event log protection	Event logs MUST be protected from: modification; unauthorised access; and whole or partial loss within the defined retention period.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	
16.6.12.C.01	Event log protection	Event logs MUST be protected from: modification; unauthorised access; and whole or partial loss within the defined retention period.	Functional	Intersects With	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.	5	
16.6.12.C.02	Event log protection	Agencies MUST configure systems to save event logs to separate secure servers as soon as possible after each event occurs.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	
16.6.12.C.02	Event log protection	Agencies MUST configure systems to save event logs to separate secure servers as soon as possible after each event occurs.	Functional	Intersects With	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.	5	
16.6.12.C.03	Event log protection	Agencies SHOULD ensure that: systems are configured to save event logs to a separate secure log server; and event log data is archived in a manner that maintains its integrity.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	
16.6.12.C.03	Event log protection	Agencies SHOULD ensure that: systems are configured to save event logs to a separate secure log server; and event log data is archived in a manner that maintains its integrity.	Functional	Intersects With	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
16.6.13.C.01	Event log archives	Event logs MUST be archived and retained for an appropriate period as determined by the agency.	Functional	Intersects With	Event Log Storage Capacity	MON-04	Mechanisms exist to allocate and proactively manage sufficient event log storage capacity to reduce the likelihood of such capacity being exceeded.	5	
16.6.13.C.01	Event log archives	Event logs MUST be archived and retained for an appropriate period as determined by the agency.	Functional	Intersects With	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	5	
16.6.13.C.01	Event log archives	Event logs MUST be archived and retained for an appropriate period as determined by the agency.	Functional	Intersects With	Event Log Backup on Separate Physical Systems / Components	MON-08.1	Mechanisms exist to back up event logs onto a physically different system or system component than the Security Incident Event Manager (SIEM) or similar automated tool.	5	
16.6.13.C.02	Event log archives	Disposal or archiving of DNS, proxy, event, systems and other operational logs MUST be in accordance with the provisions of the relevant legislation.	Functional	Intersects With	Event Log Storage Capacity	MON-04	Mechanisms exist to allocate and proactively manage sufficient event log storage capacity to reduce the likelihood of such capacity being exceeded.	5	
16.6.13.C.02	Event log archives	Disposal or archiving of DNS, proxy, event, systems and other operational logs MUST be in accordance with the provisions of the relevant legislation.	Functional	Intersects With	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	5	
16.6.13.C.02	Event log archives	Disposal or archiving of DNS, proxy, event, systems and other operational logs MUST be in accordance with the provisions of the relevant legislation.	Functional	Intersects With	Event Log Backup on Separate Physical Systems / Components	MON-08.1	Mechanisms exist to back up event logs onto a physically different system or system component than the Security Incident Event Manager (SIEM) or similar automated tool.	5	
16.6.13.C.03	Event log archives	Agencies SHOULD seek advice and determine if their logs are subject to legislation.	Functional	Intersects With	Event Log Storage Capacity	MON-04	Mechanisms exist to allocate and proactively manage sufficient event log storage capacity to reduce the likelihood of such capacity being exceeded.	5	
16.6.13.C.03	Event log archives	Agencies SHOULD seek advice and determine if their logs are subject to legislation.	Functional	Intersects With	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	5	
16.6.13.C.03	Event log archives	Agencies SHOULD seek advice and determine if their logs are subject to legislation.	Functional	Intersects With	Event Log Backup on Separate Physical Systems / Components	MON-08.1	Mechanisms exist to back up event logs onto a physically different system or system component than the Security Incident Event Manager (SIEM) or similar automated tool.	5	
16.6.13.C.04	Event log archives	Agencies SHOULD retain DNS, proxy and event logs for a minimum of 12 months.	Functional	Intersects With	Event Log Storage Capacity	MON-04	Mechanisms exist to allocate and proactively manage sufficient event log storage capacity to reduce the likelihood of such capacity being exceeded.	5	
16.6.13.C.04	Event log archives	Agencies SHOULD retain DNS, proxy and event logs for a minimum of 12 months.	Functional	Intersects With	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	5	
16.6.13.C.04	Event log archives	Agencies SHOULD retain DNS, proxy and event logs for a minimum of 12 months.	Functional	Intersects With	Event Log Backup on Separate Physical Systems / Components	MON-08.1	Mechanisms exist to back up event logs onto a physically different system or system component than the Security Incident Event Manager (SIEM) or similar automated tool.	5	
16.6.13.C.05	Event log archives	Agencies should prioritise their log retention requirements based on the risks surrounding their most sensitive systems.	Functional	Intersects With	Event Log Retention	MON-10	Mechanisms exist to retain event logs for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	5	
16.6.14.C.01	Event log auditing	Agencies MUST develop and document event log audit requirements covering: the scope of audits; the audit schedule; action to be taken when violations are detected; reporting requirements; and roles and specific responsibilities.	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	5	
16.6.15.C.01	Event log monitoring	Agencies SHOULD have a monitoring solution implemented that enables detection of incidents as they occur so that appropriate responses can be taken in adequate timeframes.	Functional	Intersects With	Automated Tools for Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation.	5	
16.6.15.C.02	Event log monitoring	Agencies SHOULD have systems available for processing system event logs to identify and correlate events which indicate behavioural anomalies or potential security compromise in the systems, in a near real-time manner.	Functional	Intersects With	Automated Tools for Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation.	5	
16.7.41.C.01	Risk Analysis	Agencies MUST undertake a risk analysis before designing and implementing MFA.	Functional	Intersects With	Assessments	IAO-02	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	
16.7.42.C.01	System Architecture and Security Controls	Where an agency has external facing systems, cloud-based services, or is authenticating to third-party services services, they MUST: require MFA for all user accounts; and implement a secure, multi-factor process to allow entities to reset their standard user credentials.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
16.7.42.C.01	System Architecture and Security Controls	Where an agency has external facing systems, cloud-based services, or is authenticating to third-party services services, they MUST: require MFA for all user accounts; and implement a secure, multi-factor process to allow entities to reset their standard user credentials.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5	
16.7.42.C.02	System Architecture and Security Controls	Where an agency has implemented MFA they MUST: require MFA for administrative or other high privileged users; and implement a secure, multi-factor process to allow entities to reset their standard user credentials.	Functional	Intersects With	Network Access to Privileged Accounts	IAC-06.1	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.	5	
16.7.42.C.03	System Architecture and Security Controls	Agencies MUST implement MFA on all user accounts with remote access to organisational resources.	Functional	Intersects With	Network Access to Privileged Accounts	IAC-06.1	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.	5	
16.7.42.C.03	System Architecture and Security Controls	Agencies MUST implement MFA on all user accounts with remote access to organisational resources.	Functional	Intersects With	Network Access to Non-Privileged Accounts	IAC-06.2	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for non-privileged accounts.	5	
16.7.42.C.04	System Architecture and Security Controls	Agencies SHOULD implement MFA on all user accounts with access to organisational resources.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5	
16.7.42.C.05	System Architecture and Security Controls	Where agencies have implemented MFA, they SHOULD implement phishing-resistant MFA on administration accounts.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5	
16.7.42.C.06	System Architecture and Security Controls	Agencies SHOULD use phishing-resistant MFA when authenticating users to systems.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5	
16.7.42.C.07	System Architecture and Security Controls	The design of an agency MFA SHOULD include consideration of: Risk identification; Level of security and access control appropriate for each aspect of an organisations information systems (data, devices, equipment, storage, cloud, etc.) A formal authorisation process for user system access and entitlements; Logging, monitoring and reporting of activity; Review of logs for orphaned accounts and inappropriate user access including unsuccessful authentication; Identification of error and anomalies which may indicate inappropriate or malicious activity; Incident response; Remediation of errors; Suspension and/or revocation of access rights where policy violations occur; Capacity planning.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
16.7.43.C.01	Integration with Policy	The design of an organisations MFA system SHOULD be integrated with the agency's Information Security Policy, the agency's Privileged Access Management (PAM) Policy, and any additional agency password policies.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5	
16.7.44.C.01	User Training	When agencies implement MFA they MUST ensure users have an understanding of the risks, and include appropriate usage and safeguards for MFA in the organisations user training and awareness programmes.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5	
17.1.51.C.01	Using cryptographic products	Agencies using cryptographic functionality within a product to protect the confidentiality, authentication, non-repudiation or integrity of information, MUST ensure that the product has completed a cryptographic evaluation recognised by the GCSB.	Functional	Intersects With	Public Key Infrastructure (PKI)	CRY-08	Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service provider.	5	
17.1.51.C.01	Using cryptographic products	Agencies using cryptographic functionality within a product to protect the confidentiality, authentication, non-repudiation or integrity of information, MUST ensure that the product has completed a cryptographic evaluation recognised by the GCSB.	Functional	Intersects With	Availability	CRY-08.1	Resiliency mechanisms exist to ensure the availability of data in the event of the loss of cryptographic keys.	5	
17.1.51.C.01	Using cryptographic products	Agencies using cryptographic functionality within a product to protect the confidentiality, authentication, non-repudiation or integrity of information, MUST ensure that the product has completed a cryptographic evaluation recognised by the GCSB.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
17.1.52.C.01	Data recovery	Cryptographic products MUST provide a means of data recovery to allow for recovery of data in circumstances where the encryption key is unavailable due to loss, damage or failure.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.1.52.C.02	Data recovery	Cryptographic products SHOULD provide a means of data recovery to allow for recovery of data in circumstances where the encryption key is unavailable due to loss, damage or failure.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.1.53.C.01	Reducing storage and physical transfer requirements	Encryption used to reduce storage or physical handling protection requirements MUST be an approved cryptographic algorithm in an EAL2 (or higher) encryption product.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.1.53.C.02	Reducing storage and physical transfer requirements	If an agency wishes to reduce the storage or physical transfer requirements for IT equipment or media that contains classified information, they MUST encrypt the classified information using High Assurance Cryptographic Equipment (HACE). It is important to note that the classification of the information itself remains unchanged.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.1.53.C.03	Reducing storage and physical transfer requirements	If an agency wishes to use encryption to reduce the storage, handling or physical transfer requirements for IT equipment or media that contains classified information, they MUST use: full disk encryption; or partial disk encryption where the access control will allow writing ONLY to the encryoted partition holding the classified information.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.1.53.C.04	Reducing storage and physical transfer requirements	If an agency wishes to use encryption to reduce the storage or physical transfer requirements for IT equipment or media that contains classified information, they SHOULD use: full disk encryption; or partial disk encryption where the access control will allow writing ONLY to the encrypted partition holding the classified information.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.1.54.C.01	Encrypting NZEO information at rest	Agencies MUST use an Approved Cryptographic Algorithm to protect NZEO information when at rest on a system.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.1.55.C.01	Information and Systems Protection	Agencies MUST use HACE if they wish to communicate or pass information over UNCLASSIFIED, insecure or unprotected networks.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.1.55.C.02	Information and Systems Protection	Information or systems classified RESTRICTED or SENSITIVE MUST be encrypted with an Approved Cryptographic Algorithm and Protocol if information is transmitted or systems are communicating over insecure or unprotected networks, such as the Internet, public networks or non-agency controlled networks.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.1.55.C.03	Information and Systems Protection	Agencies MUST encrypt aggregated agency data using an approved algorithm and protocol over insecure or unprotected networks such as the Internet, public infrastructure or non-agency controlled networks when the compromise of the aggregated data would present a significant impact to the agency.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.1.55.C.04	Information and Systems Protection	Agencies SHOULD encrypt agency data using an approved algorithm and protocol if they wish to communicate over insecure or unprotected networks such as the Internet, public networks or non-agency controlled networks.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.1.56.C.01	IT equipment using Encryption	When IT equipment storing encrypted information is turned on and authenticated, it MUST be treated as per the original classification of the information.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.1.56.C.02	IT equipment using Encryption	Agencies MUST consult the GCSB for further advice on the powered off status and treatment of specific software, systems and IT equipment.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.1.57.C.01	Encrypting NZEO information in transit	In addition to any encryption already in place for communication mediums, agencies MUST use an Approved Cryptographic Protocol and Algorithm to protect NZEO information when in transit.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.1.58.C.01	Key Refresh and Retirement	Agencies SHOULD establish cryptoperiods for all keys and cryptographic implementations in their systems and operations.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
17.1.58.C.02	Key Refresh and Retirement	Agencies SHOULD use risk assessment techniques and guidance to establish cryptoperiods.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
17.1.58.C.03	Key Refresh and Retirement	Agencies using HACE MUST consult the GCSB for key management requirements.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
17.2.17.C.01	Using Approved Cryptographic Algorithms	Agencies MUST ensure that only Approved Cryptographic Algorithms can be used when using an unevaluated product that implements a combination of approved and non-approved Cryptographic Algorithms.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.2.18.C.01	Approved asymmetric/public key algorithms	Agencies SHOULD use ECDH and ECDSA for all new systems, version upgrades and major system modifications.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.2.19.C.01	Using DH	Agencies using DH, for the approved use of agreeing on encryption session keys, MUST use a modulus of at least 3072 bits.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.2.20.C.01	Equipment using DH	Devices which are NOT capable of implementing required key lengths MUST be reconfigured with the longest feasible key length as a matter of urgency.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.2.20.C.02	Equipment using DH	Devices which are NOT capable of implementing required key lengths MUST be scheduled for replacement as a matter of urgency.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.2.21.C.01	Using DSA (for legacy use only)	Agencies using DSA, for the approved use of digital signatures, MUST use a modulus of at least 1024 bits.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.2.22.C.01	Using ECDH	Agencies using ECDH, for the approved use of agreeing on encryption session keys, MUST implement the curve P-384 (prime moduli).	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.2.22.C.02	Using ECDH	All VPNs using an ECDH key length less than 384 MUST replace all Pre-Shared Keys with keys of at least 384 bits, as soon as possible.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.2.23.C.01	Using ECDSA	Agencies using ECDSA, for the approved use of digital signatures, MUST implement the curve P-384 (prime moduli).	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.2.24.C.01	Using RSA	Agencies using RSA, for the approved use of digital signatures and passing encryption session keys or similar keys, MUST use a modulus of at least 3072 bits.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
17.2.24.C.02	Using RSA	Agencies using RSA, for the approved use of digital signatures and passing encryption session keys or similar keys, MUST ensure that the public keys used for passing encrypted session keys are different to the keys used for digital signatures.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.2.24.C.03	Using RSA	Agencies using RSA, for the approved use of digital signatures and passing encryption session keys or similar keys, SHOULD use a modulus of at least 4096 bits.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.2.25.C.01	Public key infrastructure using RSA	Agencies using RSA keys within internet X.509 Public Key Infrastructure certificates MUST use a modulus of at least 2048 bits.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.2.26.C.01	Approved hashing algorithms	Agencies MUST use the SHA-2 family for new systems. Use of SHA-1 is permitted ONLY for legacy systems.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.2.26.C.02	Approved hashing algorithms	Agencies MUST use a minimum of SHA-384 when using hashing algorithms to provide integrity protection for information classified as RESTRICTED/SENSITIVE or above.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.2.26.C.03	Approved hashing algorithms	In all other cases when information requires integrity protection using hashing algorithms, Agencies MUST use a minimum of SHA-256.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.2.27.C.01	Salts	Memorised secrets such as passwords MUST be stored in a form that is resistant to offline attacks.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.2.27.C.02	Salts	Memorised secrets such as passwords SHOULD be salted and hashed using a suitable one-way key derivation function. See 17.2.14.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.2.27.C.03	Salts	The salt SHOULD be at least 32 bits in length, be chosen arbitrarily, and each instance is unique so as to minimise salt value collisions among stored hashes.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.2.28.C.01	Approved symmetric encryption algorithms	Agencies using approved symmetric encryption algorithms (e.g. AES) SHOULD NOT use Electronic Code Book (ECB) mode.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.3.6.C.01	Using Approved Cryptographic Protocols	Agencies using a product that implements an Approved Cryptographic Protocol MUST ensure that only Approved Cryptographic Protocols can be used.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.4.16.C.01	Using TLS	Agencies SHOULD use the current version of TLS (version 1.3).	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.4.16.C.02	Using TLS	Agencies SHOULD NOT use any version of SSL.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.5.6.C.01	Using SSH	The table below outlines the settings that SHOULD be implemented when using SSH. Configuration description Configuration directive Disallow the use of SSH version 1 Protocol 2 On machines with multiple interfaces, configure the SSH daemon to listen only on the required interfaces ListenAddress xxx.xxx.xxx.xxx Disable connection forwarding AllowTCPForwarding no Disable gateway ports Gatewayports no Disable the ability to login directly as root PermitRootLogin no Disable host-based authentication HostbasedAuthentication no Disable rhosts-based authentication RhostsAuthentication no IgnoreRhosts yes Do not allow empty passwords PermitEmptyPasswords no Configure a suitable login banner Banner/directory/filename Configure a login authentication timeout of no more than 60 seconds LoginGraceTime xx Disable X forwarding X11Forwarding no	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.5.6.C.01	Using SSH	The table below outlines the settings that SHOULD be implemented when using SSH. Configuration description Configuration directive Disallow the use of SSH version 1 Protocol 2 On machines with multiple interfaces, configure the SSH daemon to listen only on the required interfaces ListenAddress xxx.xxx.xxx.xxx Disable connection forwarding AllowTCPForwarding no Disable gateway ports Gatewayports no Disable the ability to login directly as root PermitRootLogin no Disable host-based authentication HostbasedAuthentication no Disable rhosts-based authentication RhostsAuthentication no IgnoreRhosts yes Do not allow empty passwords PermitEmptyPasswords no Configure a suitable login banner Banner/directory/filename Configure a login authentication timeout of no more than 60 seconds LoginGraceTime xx Disable X forwarding X11Forwarding no	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	
17.5.7.C.01	Authentication mechanisms	Agencies SHOULD use public key-based authentication before using password-based authentication.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	
17.5.7.C.02	Authentication mechanisms	Agencies that allow password authentication SHOULD use techniques to block brute force attacks against the password.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	
17.5.8.C.01	Automated remote access	Agencies SHOULD use parameter checking when using the "forced command" option.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	
17.5.8.C.02	Automated remote access	Agencies that use logins without a password for automated purposes SHOULD disable: access from IP addresses that do not need access; port forwarding; agent credential forwarding; X11 display remoting; and console access.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	
17.5.8.C.03	Automated remote access	Agencies that use remote access without the use of a password SHOULD use the "forced command" option to specify what command is executed.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	
17.5.9.C.01	SSH-agent	Agencies that use SSH-agent or other similar key caching programs SHOULD: only use the software on workstation and servers with screenlocks; ensure that the key cache expires within four hours of inactivity; and ensure that agent credential forwarding is used when multiple SSH traversal is needed.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
17.5.10.C.01	SSH-Versions	Agencies SHOULD ensure that the latest implementation of SSH software is being used. Older versions contain known vulnerabilities.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	
17.6.6.C.01	Decommissioning	Decommissioning of faulty or redundant equipment MUST comply with media sanitisation requirements described in Chapter 12 - Product Security.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
17.6.6.C.01	Decommissioning	Decommissioning of faulty or redundant equipment MUST comply with media sanitisation requirements described in Chapter 12 - Product Security.	Functional	Intersects With	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
17.6.7.C.01	Using S/MIME	Agencies MUST NOT allow versions of S/MIME earlier than 3.0 to be used.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.6.7.C.01	Using S/MIME	Agencies MUST NOT allow versions of S/MIME earlier than 3.0 to be used.	Functional	Intersects With	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
17.7.6.C.01	Using OpenPGP Message Format	Agencies MUST immediately revoke key pairs when a private certificate is suspected of being compromised or leaves the control of the agency.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.8.10.C.01	Mode of operation	Agencies SHOULD use tunnel mode for IPSec connections.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.8.10.C.02	Mode of operation	Agencies choosing to use transport mode SHOULD additionally use an IP tunnel for IPSec connections.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.8.11.C.01	Protocol	Agencies SHOULD use the ESP protocol for IPSec connections.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.8.12.C.01	ISAKMP modes	Agencies using ISAKMP SHOULD disable aggressive mode for IKE.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.8.13.C.01	Security association lifetimes	Agencies SHOULD use a security association lifetime of four hours or 14400 seconds, or less.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.8.14.C.01	HMAC algorithms	Agencies SHOULD use HMAC-SHA256, HMAC-SHA384 or HMAC-SHA512 as the HMAC algorithm.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.8.15.C.01	DH groups	Agencies SHOULD use the largest modulus size available for the DH exchange.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.8.16.C.01	Perfect Forward Secrecy	Agencies SHOULD use Perfect Forward Secrecy for IPSec connections.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.8.17.C.01	IKE Extended Authentication	Agencies SHOULD disable the use of XAUTH for IPSec connections using IKEv1.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.9.30.C.01	Developing key management plans	Agencies SHOULD assess the risks associated around key ownership, possession, and control against their own security and business requirements.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.9.30.C.02	Developing key management plans	Agencies SHOULD develop a KMP when they have implemented a cryptographic system using commercial grade cryptographic equipment.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.9.30.C.03	Developing key management plans	The level of detail included in a KMP MUST be consistent with the criticality and classification of the information to be protected.	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5	
17.9.31.C.01	Contents of key management plans	The table below describes the minimum contents which SHOULD be documented in the KMP. Topic Content Objectives Objectives of the cryptographic system and KMP, including organisational aims. Refer to relevant NZCSIs. System description The environment. Maximum classification of information protected. Topology diagram(s) and description of the cryptographic system topology including data flows. The use of keys. Key algorithm. Key length. Key lifetime. Roles and administrative responsibilities Documents roles and responsibilities, including, if relevant, the COMSEC custodian, cryptographic systems administrator, record keeper, cloud service provider, and auditor. Accounting How accounting will be undertaken for the cryptographic system. What records will be maintained. How records will be audited. Classification Classification of the cryptographic system hardware. Classification of cryptographic system software. Classification of the cryptographic system documentation. Information security incidents	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.9.32.C.01	Accounting	Agencies MUST be able to readily account for all transactions relating to cryptographic system material including identifying hardware and all software versions issued with the equipment and materials, including date and place of issue.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.9.32.C.02	Accounting	Agencies SHOULD be able to readily account for all transactions relating to cryptographic system material including identifying hardware and all software versions issued with the equipment and materials, including date and place of issue.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.9.33.C.01	Audits, compliance and inventory checks	Agencies MUST conduct audits using two personnel with cryptographic system administrator access.	Functional	Intersects With	Periodic Audits	CPL-02.2	Mechanisms exist to conduct periodic audits of security, compliance and resilience controls to evaluate conformity with the organization's documented policies, standards and procedures.	5	
17.9.33.C.02	Audits, compliance and inventory checks	Agencies SHOULD conduct audits of cryptographic system material: on handover/takeover of administrative responsibility for the cryptographic system; on change of personnel with access to the cryptographic system; and at least annually.	Functional	Intersects With	Periodic Audits	CPL-02.2	Mechanisms exist to conduct periodic audits of security, compliance and resilience controls to evaluate conformity with the organization's documented policies, standards and procedures.	5	
17.9.33.C.03	Audits, compliance and inventory checks	Agencies SHOULD perform audits to: account for all cryptographic system material; and confirm that agreed security measures documented in the KMP are being followed.	Functional	Intersects With	Periodic Audits	CPL-02.2	Mechanisms exist to conduct periodic audits of security, compliance and resilience controls to evaluate conformity with the organization's documented policies, standards and procedures.	5	
17.9.34.C.01	Access register	Agencies MUST hold and maintain an access register that records cryptographic system information such as: details of personnel with system administrator access; details of those whose system administrator access was withdrawn; details of system documents; accounting activities; and audit activities.	Functional	Intersects With	Cryptographic Cipher Suites and Protocols Inventory	CRY-01.5	Mechanisms exist to identify, document and review deployed cryptographic cipher suites and protocols to proactively respond to industry trends regarding the continued viability of utilized cryptographic cipher suites and protocols.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
17.9.35.C.01	Cryptographic system administrator access	Before personnel are granted cryptographic system administrator access, agencies MUST ensure that they have: a demonstrated need for access; read and agreed to comply with the relevant Key Management Policy and Plan (KMP) for the cryptographic system they are using; a security clearance at least equal to the highest classification of information processed by the cryptographic system; agreed to protect the authentication information for the cryptographic system at the highest classification of information it secures; agreed not to share authentication information for the cryptographic system without approval; agreed to be responsible for all actions under their accounts; agreed to report all potentially security related problems to the GCSB; and ensure relevant staff have received appropriate training.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
17.9.36.C.01	Area security and access control	Cryptographic system equipment SHOULD be stored in a room that meets the requirements for a server room of an appropriate level based on the classification of information the cryptographic system processes.	Functional	Intersects With	Security of Assets & Media	AST-05	Mechanisms exist to maintain strict control over Technology Assets, Applications, Services and/or Data (TAASD) to preserve confidentiality and integrity.	5	
17.9.36.C.02	Area security and access control	Areas in which cryptographic system material is used SHOULD be separated from other areas and designated as a controlled cryptography area.	Functional	Intersects With	Working in Secure Areas	PES-04.1	Physical security mechanisms exist to allow only authorized personnel access to secure areas.	5	
17.9.37.C.01	High assurance cryptographic equipment	Agencies MUST comply with NZCSI when using HACE.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
17.9.38.C.01	Transporting commercial grade cryptographic equipment & products	Unkeyed commercial grade cryptographic equipment MUST be distributed and managed by a means approved for the transportation and management of government property.	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5	
17.9.38.C.02	Transporting commercial grade cryptographic equipment & products	Keyed commercial grade cryptographic equipment MUST be distributed, managed and stored by a means approved for the transportation and management of government property based on the classification of the key within the equipment.	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5	
17.9.38.C.03	Transporting commercial grade cryptographic equipment & products	Agencies SHOULD NOT transport commercial grade cryptographic equipment or products in a keyed state.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
17.10.12.C.01	Hardware Security Modules	Agencies MUST consider the use of HSMs when undertaking a security risk assessment or designing network and security architectures.	Functional	Intersects With	Hardware Security Modules (HSM)	IAC-12.1	Automated mechanisms exist to utilize Hardware Security Modules (HSM) to protect authenticators on which the component relies.	5	
17.10.12.C.02	Hardware Security Modules	Agencies MUST follow the product selection guidance in this manual. See Chapter 12 - Product Security.	Functional	Intersects With	Hardware Security Modules (HSM)	IAC-12.1	Automated mechanisms exist to utilize Hardware Security Modules (HSM) to protect authenticators on which the component relies.	5	
17.10.12.C.03	Hardware Security Modules	Agencies SHOULD consider the use of HSMs when undertaking a security risk assessment or designing network and security architectures.	Functional	Intersects With	Hardware Security Modules (HSM)	IAC-12.1	Automated mechanisms exist to utilize Hardware Security Modules (HSM) to protect authenticators on which the component relies.	5	
17.10.12.C.04	Hardware Security Modules	Agencies SHOULD follow the product selection guidance in this manual. See Chapter 12 - Product Security.	Functional	Intersects With	Hardware Security Modules (HSM)	IAC-12.1	Automated mechanisms exist to utilize Hardware Security Modules (HSM) to protect authenticators on which the component relies.	5	
18.1.9.C.01	Classification of Network Documentation	Agencies MUST perform a security risk assessment before providing network documentation to a third party, such as a commercial provider or contractor.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
18.1.9.C.02	Classification of Network Documentation	Systems documentation and detailed network diagrams MUST be classified at least to the level of classification of the data to be carried on those systems.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive and/or regulated data flows.	5	
18.1.9.C.02	Classification of Network Documentation	Systems documentation and detailed network diagrams MUST be classified at least to the level of classification of the data to be carried on those systems.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
18.1.9.C.03	Classification of Network Documentation	Network documentation provided to a third party, such as to a commercial provider or contractor, MUST contain only the information necessary for them to undertake their contractual services and functions, consistent with the need-to-know principle.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
18.1.9.C.04	Classification of Network Documentation	Detailed network configuration information MUST NOT be published in tender documentation.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
18.1.9.C.05	Classification of Network Documentation	Security aspects SHOULD be considered when determining the classification level of systems and network documentation.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
18.1.10.C.01	Configuration management	Agencies SHOULD keep the network configuration under the control of a network management authority.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
18.1.10.C.01	Configuration management	Agencies SHOULD keep the network configuration under the control of a network management authority.	Functional	Intersects With	Development & Test Environment Configurations	CFG-02.4	Mechanisms exist to manage baseline configurations for development and test environments separately from operational baseline configurations to minimize the risk of unintentional changes.	5	
18.1.10.C.01	Configuration management	Agencies SHOULD keep the network configuration under the control of a network management authority.	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	5	
18.1.10.C.01	Configuration management	Agencies SHOULD keep the network configuration under the control of a network management authority.	Functional	Intersects With	Network Device Configuration File Synchronization	CFG-02.6	Mechanisms exist to configure network devices to synchronize startup and running configuration files.	5	
18.1.10.C.02	Configuration management	All changes to the configuration SHOULD be documented and approved through a formal change control process.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
18.1.10.C.02	Configuration management	All changes to the configuration SHOULD be documented and approved through a formal change control process.	Functional	Intersects With	Development & Test Environment Configurations	CFG-02.4	Mechanisms exist to manage baseline configurations for development and test environments separately from operational baseline configurations to minimize the risk of unintentional changes.	5	
18.1.10.C.02	Configuration management	All changes to the configuration SHOULD be documented and approved through a formal change control process.	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	5	
18.1.10.C.02	Configuration management	All changes to the configuration SHOULD be documented and approved through a formal change control process.	Functional	Intersects With	Network Device Configuration File Synchronization	CFG-02.6	Mechanisms exist to configure network devices to synchronize startup and running configuration files.	5	
18.1.10.C.03	Configuration management	Agencies SHOULD regularly review their network configuration to ensure that it conforms to the documented network configuration.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
18.1.10.C.03	Configuration management	Agencies SHOULD regularly review their network configuration to ensure that it conforms to the documented network configuration.	Functional	Intersects With	Development & Test Environment Configurations	CFG-02.4	Mechanisms exist to manage baseline configurations for development and test environments separately from operational baseline configurations to minimize the risk of unintentional changes.	5	
18.1.10.C.03	Configuration management	Agencies SHOULD regularly review their network configuration to ensure that it conforms to the documented network configuration.	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	5	
18.1.10.C.03	Configuration management	Agencies SHOULD regularly review their network configuration to ensure that it conforms to the documented network configuration.	Functional	Intersects With	Network Device Configuration File Synchronization	CFG-02.6	Mechanisms exist to configure network devices to synchronize startup and running configuration files.	5	
18.1.10.C.04	Configuration management	Agencies SHOULD deploy an automated tool that compares the running configuration of network devices against the documented configuration.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
18.1.10.C.04	Configuration management	Agencies SHOULD deploy an automated tool that compares the running configuration of network devices against the documented configuration.	Functional	Intersects With	Development & Test Environment Configurations	CFG-02.4	Mechanisms exist to manage baseline configurations for development and test environments separately from operational baseline configurations to minimize the risk of unintentional changes.	5	
18.1.10.C.04	Configuration management	Agencies SHOULD deploy an automated tool that compares the running configuration of network devices against the documented configuration.	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	5	
18.1.10.C.04	Configuration management	Agencies SHOULD deploy an automated tool that compares the running configuration of network devices against the documented configuration.	Functional	Intersects With	Network Device Configuration File Synchronization	CFG-02.6	Mechanisms exist to configure network devices to synchronize startup and running configuration files.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
18.1.11.C.01	Network diagrams	For each network an agency manages they MUST have: a high-level diagram showing all connections and gateways into the network; and a network diagram showing all communications equipment.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive and/or regulated data flows.	5	
18.1.12.C.01	Updating network diagrams	An agency's network diagrams MUST: be updated as network changes are made; and include a â€¯Current as at [date] statement on each page.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive and/or regulated data flows.	5	
18.1.12.C.02	Updating network diagrams	An agency's network diagrams SHOULD: be updated as network changes are made; and include a â€¯Current as at [date] statement on each page.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive and/or regulated data flows.	5	
18.1.13.C.01	Limiting network access	Agencies MUST implement network access controls on all 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	
18.1.13.C.01	Limiting network access	Agencies MUST implement network access controls on all networks.	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, permit by exception).	5	
18.1.13.C.02	Limiting network access	Agencies SHOULD implement network access controls on all 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	
18.1.13.C.02	Limiting network access	Agencies SHOULD implement network access controls on all networks.	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, permit by exception).	5	
18.1.14.C.01	Management traffic	Agencies SHOULD implement protection measures to minimise the risk of unauthorised access to network management traffic on a network.	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	
18.1.14.C.01	Management traffic	Agencies SHOULD implement protection measures to minimise the risk of unauthorised access to network management traffic on a network.	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, permit by exception).	5	
18.1.15.C.01	Simple Network Management IT Protocol (SNMP)	Agencies SHOULD NOT use SNMP unless a specific requirement exists.	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5	
18.1.15.C.01	Simple Network Management IT Protocol (SNMP)	Agencies SHOULD NOT use SNMP unless a specific requirement exists.	Functional	Intersects With	Ports, Protocols & Services In Use	TDA-02.1	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to identify early in the Secure Development Life Cycle (SDLC), the functions, ports, protocols and services intended for use.	5	
18.1.15.C.02	Simple Network Management IT Protocol (SNMP)	Agencies SHOULD implement SNMPv3 where a specific SNMP requirement exists.	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5	
18.1.15.C.02	Simple Network Management IT Protocol (SNMP)	Agencies SHOULD implement SNMPv3 where a specific SNMP requirement exists.	Functional	Intersects With	Ports, Protocols & Services In Use	TDA-02.1	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to identify early in the Secure Development Life Cycle (SDLC), the functions, ports, protocols and services intended for use.	5	
18.1.15.C.03	Simple Network Management IT Protocol (SNMP)	Agencies SHOULD change all default community strings in SNMP implementations.	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5	
18.1.15.C.03	Simple Network Management IT Protocol (SNMP)	Agencies SHOULD change all default community strings in SNMP implementations.	Functional	Intersects With	Ports, Protocols & Services In Use	TDA-02.1	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to identify early in the Secure Development Life Cycle (SDLC), the functions, ports, protocols and services intended for use.	5	
18.1.15.C.04	Simple Network Management IT Protocol (SNMP)	SNMP access SHOULD be configured as read-only.	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5	
18.1.15.C.04	Simple Network Management IT Protocol (SNMP)	SNMP access SHOULD be configured as read-only.	Functional	Intersects With	Ports, Protocols & Services In Use	TDA-02.1	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to identify early in the Secure Development Life Cycle (SDLC), the functions, ports, protocols and services intended for use.	5	
18.2.5.C.01	Bridging networks	Devices MUST NOT be configured to remember and automatically connect to any wireless networks that they have previously connected to.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
18.2.5.C.02	Bridging networks	Wireless auto-connect functionality on devices SHOULD be disabled, preferably by a hardware switch, whenever connected to a fixed network.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
18.2.6.C.01	Providing wireless communications for public access	Agencies deploying a wireless network for public access MUST separate it from any other agency networks; including BYOD networks.	Functional	Intersects With	Guest Networks	NET-02.2	Mechanisms exist to implement and manage a secure guest network.	5	
18.2.6.C.01	Providing wireless communications for public access	Agencies deploying a wireless network for public access MUST separate it from any other agency networks; including BYOD networks.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
18.2.7.C.01	Using wireless communications	Agencies MUST NOT use wireless networks unless the security of the agency's wireless deployment has been approved by GCSB.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
18.2.8.C.01	Selecting wireless access point equipment	All wireless access points used for government wireless networks MUST be Wi-Fi Alliance certified.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
18.2.9.C.01	802.1X Authentication	EAP-TLS or PEAP-EAP-TLS MUST be used on wireless networks to perform mutual authentication.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	
18.2.9.C.02	802.1X Authentication	EAP-TLS, PEAP-EAP-TLS, EAP-TTLS or PEAP MUST be used on wireless networks to perform mutual authentication.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	
18.2.10.C.01	Evaluation of 802.1X authentication implementation	Supplicants, authenticators and the authentication server used in wireless networks MUST have completed an appropriate product evaluation.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	
18.2.10.C.01	Evaluation of 802.1X authentication implementation	Supplicants, authenticators and the authentication server used in wireless networks MUST have completed an appropriate product evaluation.	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	5	
18.2.10.C.02	Evaluation of 802.1X authentication implementation	Supplicants, authenticators and the authentication server used in wireless networks SHOULD have completed an appropriate product evaluation.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	
18.2.10.C.02	Evaluation of 802.1X authentication implementation	Supplicants, authenticators and the authentication server used in wireless networks SHOULD have completed an appropriate product evaluation.	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	5	
18.2.11.C.01	Issuing certificates for authentication	Agencies MUST generate certificates using a certificate authority product or hardware security module that has completed an appropriate product evaluation.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	
18.2.11.C.01	Issuing certificates for authentication	Agencies MUST generate certificates using a certificate authority product or hardware security module that has completed an appropriate product evaluation.	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	5	
18.2.11.C.02	Issuing certificates for authentication	The certificates for both a device and user accessing a wireless network MUST NOT be stored on the same device.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	
18.2.11.C.02	Issuing certificates for authentication	The certificates for both a device and user accessing a wireless network MUST NOT be stored on the same device.	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	5	
18.2.11.C.03	Issuing certificates for authentication	Agencies SHOULD use unique certificates for both devices and users accessing a wireless network.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	
18.2.11.C.03	Issuing certificates for authentication	Agencies SHOULD use unique certificates for both devices and users accessing a wireless network.	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
18.2.11.C.04	Issuing certificates for authentication	Certificates for users accessing wireless networks SHOULD be issued on smart cards with access PINs and not stored with a device when not in use.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	
18.2.11.C.04	Issuing certificates for authentication	Certificates for users accessing wireless networks SHOULD be issued on smart cards with access PINs and not stored with a device when not in use.	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	5	
18.2.11.C.05	Issuing certificates for authentication	Certificates stored on devices accessing wireless networks SHOULD be protected by implementing full disk encryption on the devices.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	
18.2.11.C.05	Issuing certificates for authentication	Certificates stored on devices accessing wireless networks SHOULD be protected by implementing full disk encryption on the devices.	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	5	
18.2.12.C.01	Using commercial certification authorities for certificate generation	Devices MUST be configured to validate the server certificate, disable any trust for certificates generated by commercial certificate authorities that are not trusted and disable the ability to prompt users to authorise new servers or commercial certification authorities.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	
18.2.12.C.01	Using commercial certification authorities for certificate generation	Devices MUST be configured to validate the server certificate, disable any trust for certificates generated by commercial certificate authorities that are not trusted and disable the ability to prompt users to authorise new servers or commercial certification authorities.	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	5	
18.2.12.C.02	Using commercial certification authorities for certificate generation	Devices SHOULD be set to enable identity privacy.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	
18.2.12.C.02	Using commercial certification authorities for certificate generation	Devices SHOULD be set to enable identity privacy.	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	5	
18.2.13.C.01	Caching 802.1X authentication outcomes	The PMK caching period SHOULD NOT be set to greater than 1440 minutes (24 hours).	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	
18.2.13.C.01	Caching 802.1X authentication outcomes	The PMK caching period SHOULD NOT be set to greater than 1440 minutes (24 hours).	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	5	
18.2.14.C.01	Remote Authentication Dial-In User Service (RADIUS) authentication	Communications between wireless access points and a RADIUS server MUST be encapsulated with an additional layer of encryption using an approved encryption product (See Chapter 17 - Cryptography).	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	
18.2.14.C.01	Remote Authentication Dial-In User Service (RADIUS) authentication	Communications between wireless access points and a RADIUS server MUST be encapsulated with an additional layer of encryption using an approved encryption product (See Chapter 17 - Cryptography).	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	5	
18.2.15.C.01	Encryption	Agencies using wireless networks MUST ensure that classified information is protected by cryptography that meets the assurance level mandated for the communication of information over unclassified network infrastructure (See Section 17.2, Suite B).	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	
18.2.15.C.01	Encryption	Agencies using wireless networks MUST ensure that classified information is protected by cryptography that meets the assurance level mandated for the communication of information over unclassified network infrastructure (See Section 17.2, Suite B).	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	5	
18.2.16.C.01	Cipher Block Chaining Message Authentication Code Protocol (CCMP) Encryption	CCMP MUST be used to protect the confidentiality and integrity of all wireless network traffic.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	
18.2.16.C.01	Cipher Block Chaining Message Authentication Code Protocol (CCMP) Encryption	CCMP MUST be used to protect the confidentiality and integrity of all wireless network traffic.	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	5	
18.2.17.C.01	Temporal Key Integrity Protocol (TKIP) and Wireless Encryption Protocol (WEP)	TKIP and WEP support MUST be disabled or removed from wireless access points.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	
18.2.17.C.01	Temporal Key Integrity Protocol (TKIP) and Wireless Encryption Protocol (WEP)	TKIP and WEP support MUST be disabled or removed from wireless access points.	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	5	
18.2.18.C.01	Wired Equivalent Privacy (WEP)	Agencies MUST NOT use WEP for wireless deployments.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	
18.2.18.C.01	Wired Equivalent Privacy (WEP)	Agencies MUST NOT use WEP for wireless deployments.	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	5	
18.2.19.C.01	Wi-Fi Protected Access (WPA)	Agencies MUST NOT use Wi-Fi Protected Access (WPA) for wireless deployments.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	
18.2.19.C.01	Wi-Fi Protected Access (WPA)	Agencies MUST NOT use Wi-Fi Protected Access (WPA) for wireless deployments.	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	5	
18.2.19.C.02	Wi-Fi Protected Access (WPA)	Agencies SHOULD NOT use Wi-Fi Protected Access 2 (WPA2) for wireless deployments.	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	5	
18.2.19.C.03	Wi-Fi Protected Access (WPA)	Agencies SHOULD use Wi-Fi Protected Access 3 (WPA3) for wireless deployments with preference given to WPA3-Enterprise 192-bit mode.	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	5	
18.2.20.C.01	Pre-shared keys	Agencies MUST NOT use pre-shared keys for wireless authentication.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	
18.2.20.C.01	Pre-shared keys	Agencies MUST NOT use pre-shared keys for wireless authentication.	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	5	
18.2.20.C.02	Pre-shared keys	If pre-shared keys are used, agencies SHOULD use random keys of the maximum allowable length.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	
18.2.20.C.02	Pre-shared keys	If pre-shared keys are used, agencies SHOULD use random keys of the maximum allowable length.	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	5	
18.2.20.C.03	Pre-shared keys	Agencies SHOULD NOT use pre-shared keys for wireless authentication.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	
18.2.20.C.03	Pre-shared keys	Agencies SHOULD NOT use pre-shared keys for wireless authentication.	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	5	
18.2.21.C.01	Administrative interfaces for wireless access points	Agencies SHOULD disable the administrative interface on wireless access points for wireless connections.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	
18.2.21.C.01	Administrative interfaces for wireless access points	Agencies SHOULD disable the administrative interface on wireless access points for wireless connections.	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	5	
18.2.22.C.01	Protecting management frames on wireless networks	Wireless access points and devices SHOULD be upgraded to support a minimum of the 802.11w amendment.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
18.2.22.C.01	Protecting management frames on wireless networks	Wireless access points and devices SHOULD be upgraded to support a minimum of the 802.11w amendment.	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	5	
18.2.23.C.01	Default service set identifiers (SSIDs)	Agencies MUST change the default SSID of wireless access points.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	
18.2.23.C.01	Default service set identifiers (SSIDs)	Agencies MUST change the default SSID of wireless access points.	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	5	
18.2.23.C.02	Default service set identifiers (SSIDs)	Agencies MUST rename or remove default accounts and passwords.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	
18.2.23.C.02	Default service set identifiers (SSIDs)	Agencies MUST rename or remove default accounts and passwords.	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	5	
18.2.24.C.01	Changing the SSID	The SSID of a wireless network SHOULD NOT be readily associated with an agency, the premises, location or the functionality of the network.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	
18.2.24.C.01	Changing the SSID	The SSID of a wireless network SHOULD NOT be readily associated with an agency, the premises, location or the functionality of the network.	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	5	
18.2.25.C.01	SSID Broadcasting	Agencies SHOULD NOT disable SSID broadcasting on wireless networks.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	
18.2.25.C.01	SSID Broadcasting	Agencies SHOULD NOT disable SSID broadcasting on wireless networks.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
18.2.25.C.01	SSID Broadcasting	Agencies SHOULD NOT disable SSID broadcasting on wireless networks.	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	5	
18.2.26.C.01	Static addressing	Agencies SHOULD use the Dynamic Host Configuration Protocol (DHCP) for assigning IP addresses on wireless networks.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
18.2.27.C.01	Media Access Control address filtering	MAC address filtering SHOULD NOT be used as a security mechanism to restrict which devices connect to a wireless network.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
18.2.28.C.01	Documentation	Key generation, distribution and rekeying procedures SHOULD be documented in the SecPlan for the wireless network.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
18.2.28.C.02	Documentation	Wireless device drivers and their versions SHOULD be documented in the SecPlan for the wireless network.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
18.2.29.C.01	Non-agency devices connecting to agency controlled wireless networks	Where BYOD has been approved by an agency, any wireless network allowing BYOD connections MUST be segregated from all other agency networks, including any agency wireless networks.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
18.2.29.C.02	Non-agency devices connecting to agency controlled wireless networks	Any BYOD devices MUST comply with the policies and configuration described in Section 21.4â€“ BYOD.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
18.2.29.C.03	Non-agency devices connecting to agency controlled wireless networks	Agencies MUST NOT allow non-agency devices to connect to agency controlled wireless networks not intended or configured for BYOD devices or for public access.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
18.2.30.C.01	Agency devices connecting to non-agency controlled wireless networks	Agencies SHOULD NOT allow agency devices to connect to non-agency controlled wireless networks.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
18.2.31.C.01	Connecting wireless networks to fixed networks	Connections between wireless networks and fixed networks SHOULD be treated in the same way as connections between fixed networks and the Internet.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
18.2.32.C.01	Wireless network footprint and Radio Frequency (RF) Controls	Instead of deploying a small number of wireless access points that broadcast on high power, more wireless access points that use minimal broadcast power SHOULD be deployed to achieve the desired wireless network footprint.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
18.2.33.C.01	Radio Frequency (RF) Propagation & Controls	The effective range of wireless communications outside an agency's area of control SHOULD be limited by: Minimising the output power level of wireless devices. Implementing RF shielding within buildings in which wireless networks are used.	Functional	Intersects With	Wireless Boundaries	NET-15.4	Mechanisms exist to confine wireless communications to organization-controlled boundaries.	5	
18.2.34.C.01	Interference between wireless networks	Wireless networks SHOULD use channel separation.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
18.3.8.C.01	Video and voice-aware firewalls	Agencies SHOULD use a video, unified communication or voice-aware firewall that meets the same minimum level of assurance as specified for normal firewalls.	Functional	Intersects With	Voice Over Internet Protocol (VoIP) Security	AST-21	Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.	5	
18.3.9.C.01	Protecting IPT signalling and data	Agencies SHOULD protect VTC and IPT signalling and data by using encryption.	Functional	Intersects With	Voice Over Internet Protocol (VoIP) Security	AST-21	Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.	5	
18.3.9.C.02	Protecting IPT signalling and data	An encrypted and non-replayable two-way authentication scheme SHOULD be used for call authentication and authorisation.	Functional	Intersects With	Voice Over Internet Protocol (VoIP) Security	AST-21	Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.	5	
18.3.10.C.01	Establishment of secure signalling and data protocols	Agencies SHOULD ensure that VTC and IPT functions are established using only the secure signalling and data protocols.	Functional	Intersects With	Voice Over Internet Protocol (VoIP) Security	AST-21	Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.	5	
18.3.11.C.01	Local area network traffic separation	Agencies MUST either separate or segregate the VTC and IPT traffic from other data traffic.	Functional	Intersects With	Voice Over Internet Protocol (VoIP) Security	AST-21	Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.	5	
18.3.11.C.02	Local area network traffic separation	Agencies SHOULD either separate or segregate the IPT traffic from other data traffic.	Functional	Intersects With	Voice Over Internet Protocol (VoIP) Security	AST-21	Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.	5	
18.3.12.C.01	VTC and IPT Device setup	Agencies MUST: configure VTC and VoIP devices to authenticate themselves to the call controller upon registration; disable phone auto-registration and only allow an allow list of authorised devices to access the network; block unauthorised devices by default; disable all unused and prohibited functionality; and use individual logins for IP phones.	Functional	Intersects With	Voice Over Internet Protocol (VoIP) Security	AST-21	Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.	5	
18.3.12.C.02	VTC and IPT Device setup	Agencies SHOULD: configure VoIP phones to authenticate themselves to the call controller upon registration; disable phone auto-registration and use an allow list of authorised devices to access the network; block unauthorised devices by default; disable all unused and prohibited functionality; and use individual logins for IP phones.	Functional	Intersects With	Voice Over Internet Protocol (VoIP) Security	AST-21	Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.	5	
18.3.13.C.01	Call authentication and authorisation	Authentication and authorisation SHOULD be used for all actions on the IPT network, including: call setup; changing settings; and checking voice mail.	Functional	Intersects With	Voice Over Internet Protocol (VoIP) Security	AST-21	Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.	5	
18.3.13.C.02	Call authentication and authorisation	An encrypted and non-replayable two-way authentication scheme SHOULD be used for call authentication and authorisation.	Functional	Intersects With	Voice Over Internet Protocol (VoIP) Security	AST-21	Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.	5	
18.3.13.C.03	Call authentication and authorisation	Authentication SHOULD be enforced for: registering a new phone; changing phone users; changing settings; and accessing voice mail.	Functional	Intersects With	Voice Over Internet Protocol (VoIP) Security	AST-21	Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
18.3.14.C.01	VTC and IPT device connection to workstations	Agencies MUST NOT connect workstations to VTC or IPT devices unless the workstation or the device, as appropriate for the configuration, uses VLANs or similar mechanisms to maintain separation between VTC, IPT and other data traffic.	Functional	Intersects With	Video Teleconference (VTC) Security	AST-20	Mechanisms exist to implement secure Video Teleconference (VTC) capabilities on endpoint devices and in designated conference rooms, to prevent potential eavesdropping.	5	
18.3.14.C.01	VTC and IPT device connection to workstations	Agencies MUST NOT connect workstations to VTC or IPT devices unless the workstation or the device, as appropriate for the configuration, uses VLANs or similar mechanisms to maintain separation between VTC, IPT and other data traffic.	Functional	Intersects With	Voice Over Internet Protocol (VoIP) Security	AST-21	Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.	5	
18.3.14.C.02	VTC and IPT device connection to workstations	Agencies SHOULD NOT connect workstations to VTC or IPT devices unless the workstation or the device, as appropriate for the configuration, uses VLANs or similar mechanisms to maintain separation between VTC, IPT and other data traffic.	Functional	Intersects With	Video Teleconference (VTC) Security	AST-20	Mechanisms exist to implement secure Video Teleconference (VTC) capabilities on endpoint devices and in designated conference rooms, to prevent potential eavesdropping.	5	
18.3.14.C.02	VTC and IPT device connection to workstations	Agencies SHOULD NOT connect workstations to VTC or IPT devices unless the workstation or the device, as appropriate for the configuration, uses VLANs or similar mechanisms to maintain separation between VTC, IPT and other data traffic.	Functional	Intersects With	Voice Over Internet Protocol (VoIP) Security	AST-21	Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.	5	
18.3.15.C.01	Lobby and shared area IPT devices	Where an agency uses a VoIP phone in a lobby or shared area they SHOULD limit or disable the phones: ability to access data networks; functionality for voice mail and directory services; and use a separate network segment.	Functional	Intersects With	Voice Over Internet Protocol (VoIP) Security	AST-21	Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.	5	
18.3.15.C.02	Lobby and shared area IPT devices	Agencies SHOULD, where available, use traditional analogue phones in a lobby and shared areas.	Functional	Intersects With	Voice Over Internet Protocol (VoIP) Security	AST-21	Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.	5	
18.3.16.C.01	Usage of softphones, webcams and similar sound and video devices	Agencies using softphones or webcams SHOULD have separate dedicated network interface cards on the host for VTC or IPT network access to facilitate VLAN separation.	Functional	Intersects With	Voice Over Internet Protocol (VoIP) Security	AST-21	Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.	5	
18.3.16.C.02	Usage of softphones, webcams and similar sound and video devices	Agencies using softphones or webcams SHOULD install a host-based firewall on workstations utilising softphones or webcams that allows traffic only to and from a minimum number of ports.	Functional	Intersects With	Voice Over Internet Protocol (VoIP) Security	AST-21	Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.	5	
18.3.16.C.03	Usage of softphones, webcams and similar sound and video devices	Agencies SHOULD NOT use softphones or webcams.	Functional	Intersects With	Voice Over Internet Protocol (VoIP) Security	AST-21	Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.	5	
18.3.17.C.01	Workstations using USB softphones, webcams and similar sound and video devices	Agencies SHOULD use access control software to control USB ports on workstations using softphones and webcams by utilising the specific vendor and product identifier of the authorised device.	Functional	Intersects With	Voice Over Internet Protocol (VoIP) Security	AST-21	Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.	5	
18.3.18.C.01	Developing a denial of service response plan	Agencies SHOULD develop a Denial of Service response plan including: how to identify the precursors and other signs of DoS; how to diagnose the incident or attack type and attack method; how to diagnose the source of the DoS; what actions can be taken to clear the DoS; how communications can be maintained during a DoS; and report the incident.	Functional	Intersects With	Denial of Service (DoS) Protection	NET-02.1	Automated mechanisms exist to protect against or limit the effects of denial of service attacks.	5	
18.3.19.C.01	Content of a Denial of Service (DoS) response plan	A Denial of Service response plan SHOULD include monitoring and use of: router and switch logging and flow data; packet captures; proxy and call manager logs and access control lists; VTC and IPT aware firewalls and voice gateways; network redundancy; load balancing; PSTN failover; and alternative communication paths.	Functional	Intersects With	Denial of Service (DoS) Protection	NET-02.1	Automated mechanisms exist to protect against or limit the effects of denial of service attacks.	5	
18.4.7.C.01	Intrusion Detection and Prevention strategy (IDS/IPS)	Agencies MUST develop, implement and maintain an intrusion detection strategy that includes: appropriate intrusion detection mechanisms, including network-based IDS/IPSs and host-based IDS/IPSs as necessary; the audit analysis of event logs, including IDS/IPS logs; a periodic audit of intrusion detection procedures; information security awareness and training programs; a documented Incident Response Plans (IRP); and provide the capability to detect information security incidents and attempted network intrusions on gateways and provide real-time alerts.	Functional	Intersects With	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	5	
18.4.7.C.02	Intrusion Detection and Prevention strategy (IDS/IPS)	Agencies SHOULD develop, implement and maintain an intrusion detection strategy that includes: appropriate intrusion detection mechanisms, including network-based IDS/IPSs and host-based IDS/IPSs as necessary; the audit analysis of event logs, including IDS/IPS logs; a periodic audit of intrusion detection procedures; information security awareness and training programs; and a documented IRP.	Functional	Intersects With	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	5	
18.4.7.C.03	Intrusion Detection and Prevention strategy (IDS/IPS)	Agencies SHOULD ensure sufficient resources are provided for the maintenance and monitoring of IDS/IPS.	Functional	Intersects With	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	5	
18.4.8.C.01	IDS/IPSs on gateways	Agencies SHOULD deploy IDS/IPSs in all gateways between the agency's networks and unsecure public networks or BYOD wireless networks.	Functional	Intersects With	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	5	
18.4.8.C.01	IDS/IPSs on gateways	Agencies SHOULD deploy IDS/IPSs in all gateways between the agency's networks and unsecure public networks or BYOD wireless networks.	Functional	Intersects With	Inbound & Outbound Communications Traffic	MON-01.3	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	5	
18.4.8.C.01	IDS/IPSs on gateways	Agencies SHOULD deploy IDS/IPSs in all gateways between the agency's networks and unsecure public networks or BYOD wireless networks.	Functional	Intersects With	Wireless Network Monitoring	MON-01.5	Mechanisms exist to monitor wireless network segments for: (1) Rogue wireless devices; and (2) Anomalous and/or hostile activities.	5	
18.4.8.C.02	IDS/IPSs on gateways	Agencies SHOULD deploy IDS/IPSs at all gateways between the agency's networks and any network not managed by the agency.	Functional	Intersects With	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	5	
18.4.8.C.02	IDS/IPSs on gateways	Agencies SHOULD deploy IDS/IPSs at all gateways between the agency's networks and any network not managed by the agency.	Functional	Intersects With	Inbound & Outbound Communications Traffic	MON-01.3	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	5	
18.4.8.C.02	IDS/IPSs on gateways	Agencies SHOULD deploy IDS/IPSs at all gateways between the agency's networks and any network not managed by the agency.	Functional	Intersects With	Wireless Network Monitoring	MON-01.5	Mechanisms exist to monitor wireless network segments for: (1) Rogue wireless devices; and (2) Anomalous and/or hostile activities.	5	
18.4.8.C.03	IDS/IPSs on gateways	Agencies SHOULD locate IDS/IPSs within the gateway environment, immediately inside the outermost firewall.	Functional	Intersects With	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	5	
18.4.8.C.03	IDS/IPSs on gateways	Agencies SHOULD locate IDS/IPSs within the gateway environment, immediately inside the outermost firewall.	Functional	Intersects With	Inbound & Outbound Communications Traffic	MON-01.3	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	5	
18.4.8.C.03	IDS/IPSs on gateways	Agencies SHOULD locate IDS/IPSs within the gateway environment, immediately inside the outermost firewall.	Functional	Intersects With	Wireless Network Monitoring	MON-01.5	Mechanisms exist to monitor wireless network segments for: (1) Rogue wireless devices; and (2) Anomalous and/or hostile activities.	5	
18.4.9.C.01	IDS/IPS Maintenance	Agencies MUST select IDS / IPS that monitor uncharacteristic and suspicious activities.	Functional	Intersects With	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	5	
18.4.9.C.02	IDS/IPS Maintenance	When signature-based intrusion detection is used, agencies MUST keep the signatures and system patching up to date.	Functional	Intersects With	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	5	
18.4.10.C.01	Malicious code counter-measures	Agencies MUST: develop and maintain a set of policies and procedures covering how to: minimise the likelihood of malicious code being introduced into a system; prevent all unauthorised code from executing on an agency network; detect any malicious code installed on a system; make their system users aware of the agency's policies and procedures; and ensure that all instances of detected malicious code outbreaks are handled according to established procedures.	Functional	Intersects With	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
18.4.11.C.01	Configuring the IDS/IPS	In addition to agency defined configuration requirements, agencies SHOULD ensure that IDS/IPSs located inside a firewall are configured to generate a log entry, and an alert, for any information flows that contravene any rule within the firewall rule set.	Functional	Intersects With	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	5	
18.4.11.C.02	Configuring the IDS/IPS	Agencies SHOULD test IDS/IPSs rule sets prior to implementation to ensure that they perform as expected.	Functional	Intersects With	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	5	
18.4.11.C.03	Configuring the IDS/IPS	If a firewall is configured to block all traffic on a particular range of port numbers, the IDP/IPSs SHOULD inspect traffic for these port numbers and generate an alert if they are detected.	Functional	Intersects With	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	5	
18.4.12.C.01	Event management and correlation	Agencies SHOULD deploy tools for: the management and archive of security event information; and the correlation of suspicious events or events of interest across all agency networks.	Functional	Intersects With	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	5	
18.4.12.C.01	Event management and correlation	Agencies SHOULD deploy tools for: the management and archive of security event information; and the correlation of suspicious events or events of interest across all agency networks.	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	5	
18.4.13.C.01	Host-based IDS/IPSs	Agencies SHOULD install host-based IDS/IPSs on authentication, DNS, email, Web and other high value servers.	Functional	Intersects With	Host Intrusion Detection and Prevention Systems (HIDS / HIPS)	END-07	Mechanisms exist to utilize Host-based Intrusion Detection / Prevention Systems (HIDS / HIPS), or similar technologies, to monitor for and protect against anomalous host activity, including lateral movement across the network.	5	
18.4.14.C.01	Active content blocking	Agencies SHOULD use: filters to block unwanted content and exploits against applications that cannot be patched; settings within the applications to disable unwanted functionality; and digital signatures to restrict active content to trusted sources only.	Functional	Intersects With	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	5	
18.5.7.C.01	Use of dual-stack equipment	Agencies not using IPv6, but which have deployed dual-stack network devices and ICT equipment that supports IPv6, MUST disable the IPv6 functionality, unless that functionality is required.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
18.5.7.C.02	Use of dual-stack equipment	Network security devices on IPv6 or dual-stack networks MUST be IPv6 capable.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
18.5.8.C.01	Using IPv6	Agencies using IPv6 MUST conduct a security risk assessment on risks that could be introduced as a result of running a dual stack environment or transitioning completely to IPv6.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
18.5.8.C.02	Using IPv6	Agencies implementing a dual stack or wholly IPv6 network or environment MUST re-accredit their networks.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
18.5.8.C.03	Using IPv6	IPv6 tunnelling MUST be disabled on all network devices, unless explicitly required.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
18.5.8.C.04	Using IPv6	Dynamically assigned IPv6 addresses SHOULD be configured with DHCPv6 in a stateful manner and with lease information logged and logs stored in a centralised logging facility.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
18.5.9.C.01	New systems and networks	Any network defence elements and devices MUST be IPv6 aware.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
18.5.9.C.02	New systems and networks	New network devices, including firewalls, IDS and IPS, MUST be IPv6 capable.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
18.5.9.C.03	New systems and networks	Agencies SHOULD consider the use of DNSSEC.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
18.5.10.C.01	Introducing IPv6 capable equipment to gateways	IPv6 tunnelling MUST be blocked by network security devices at externally connected network boundaries.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
18.5.10.C.02	Introducing IPv6 capable equipment to gateways	Agencies deploying IPv6 equipment in their gateway but not enabling the functionality SHOULD undergo reaccreditation.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
18.5.11.C.01	Enabling IPv6 in gateways	Agencies enabling a dual-stack environment or a wholly IPv6 environment in their gateways MUST reaccredit their gateway systems.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
18.6.8.C.01	Assurance requirements	Agencies accessing a classified system and a less classified system via a peripheral switch MUST use an evaluated product with a level of assurance as indicated in the table below. High System Low system / Alternate Trust Domain Required Level of Assurance RESTRICTED UNCLASSIFIED EAL2 or PP CONFIDENTIAL UNCLASSIFIED high assurance RESTRICTED high assurance CONFIDENTIAL high assurance SECRET UNCLASSIFIED high assurance RESTRICTED high assurance CONFIDENTIAL high assurance SECRET high assurance TOP SECRET UNCLASSIFIED high assurance RESTRICTED high assurance	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive and/or regulated data wherever it is processed and/or stored.	5	
18.6.8.C.01	Assurance requirements	Agencies accessing a classified system and a less classified system via a peripheral switch MUST use an evaluated product with a level of assurance as indicated in the table below. High System Low system / Alternate Trust Domain Required Level of Assurance RESTRICTED UNCLASSIFIED EAL2 or PP CONFIDENTIAL UNCLASSIFIED high assurance RESTRICTED high assurance CONFIDENTIAL high assurance SECRET UNCLASSIFIED high assurance RESTRICTED high assurance CONFIDENTIAL high assurance SECRET high assurance TOP SECRET UNCLASSIFIED high assurance RESTRICTED high assurance	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
18.6.9.C.01	Assurance requirements for NZEO systems	Agencies accessing a system containing NZEO information and a system of the same classification that is not accredited to process NZEO information, MUST use an evaluated product with an EAL2 (or higher) or a PP level of assurance.	Functional	Intersects With	Highest Classification Level	DCH-02.1	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	

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
18.6.10.C.01	Cross-Connecting Systems with a device other than a KVM	Cross-connection of security domains and Trust Zones MUST be enabled through an approved KVM, Gateway or Cross-Domain solution only. High system Low system/ Alternate Trust Domain Level of assurance RESTRICTED & all lower classifications UNCLASSIFIED EAL2 or PP CONFIDENTIAL UNCLASSIFIED high assurance RESTRICTED high assurance CONFIDENTIAL high assurance SECRET UNCLASSIFIED high assurance RESTRICTED high assurance CONFIDENTIAL high assurance SECRET high assurance TOP SECRET UNCLASSIFIED high assurance RESTRICTED high assurance	Functional	Intersects With	System Administrative Processes	AST-26	Mechanisms exist to develop, implement and govern system administration processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining Technology Assets, Applications and/or Services (TAAS).	5	
18.7.14.C.01	Inverse split tunnel in remote access VPN systems	Agencies MUST undertake a threat and risk assessment on the use of inverse split tunnelling prior to enabling the functionality in remote access VPN systems.	Functional	Intersects With	Split Tunneling	CFG-03.4	Mechanisms exist to prevent split tunneling for remote devices unless the split tunnel is securely provisioned using organization-defined safeguards.	5	
18.7.14.C.02	Inverse split tunnel in remote access VPN systems	When providing inverse split-tunnelled access to internet based services ("directly accessed services"), the following aspects SHOULD be considered as part of the threat and risk assessment: How do directly accessed services authenticate agency device identities prior to granting access to the service? How do agency devices securely resolve internet addresses for directly accessed services? How are the communications between the devices and directly accessed services secured? How does an agency monitor and account for access made to directly accessed services? How does an agency protect devices from compromise if they are able to directly access internet based resources, or be directly accessed from the internet? How do directly accessed services authenticate the user of the agency device prior to granting access to the service (this is separate to authenticating the agency device itself)? How does an agency enforce the use of multi-factor authentication with directly accessed services? How does an agency authorise access to directly accessed services, and does this include from devices that are not authorised to connect to agency remote access services (authorisation and authentication are separate activities)? How is access to directly accessed cloud services removed when staff no longer require access or leave the agency?	Functional	Intersects With	Split Tunneling	CFG-03.4	Mechanisms exist to prevent split tunneling for remote devices unless the split tunnel is securely provisioned using organization-defined safeguards.	5	
19.1.10.C.01	Gateways involving cascaded connections	When agencies have cascaded connections between networks involving multiple gateways they MUST ensure that the assurance levels specified for network devices between the overall lowest and highest networks are met by the gateway between the highest network and the next highest network within the cascaded connection.	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	
19.1.11.C.01	Using gateways	Agencies MUST ensure that: all agency networks are protected from networks in other security domains by one or more gateways; all gateways contain mechanisms to filter or limit data flow at the network and content level to only the information necessary for business purposes; and all gateway components, discrete and virtual, are physically located within an appropriately secured server room.	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	
19.1.11.C.02	Using gateways	For gateways between networks in different security domains, any shared components MUST be managed by the system owners of the highest security domain or by a mutually agreed 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	
19.1.12.C.01	Configuration of gateways	Agencies MUST ensure that gateways: are the only communications paths into and out of internal networks; by default, deny all connections into and out of the network; allow only explicitly authorised connections; are managed via a secure path isolated from all connected networks (i.e. physically at the gateway or on a dedicated administration network); provide sufficient logging and audit capabilities to detect information security incidents, attempted intrusions or anomalous usage patterns; and provide real-time alerts.	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	
19.1.13.C.01	Operation of gateways	Agencies MUST ensure that all gateways connecting networks in different security domains: include a firewall of an appropriate assurance level on all gateways to filter and log network traffic attempting to enter the gateway; are configured to save event logs to a separate, secure log server; are protected by authentication, logging and audit of all physical access to gateway components; and have all controls tested to verify their effectiveness after any changes to their configuration.	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	
19.1.14.C.01	Demilitarised zones	Agencies MUST use demilitarised zones to house systems and information directly accessed externally.	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	
19.1.14.C.01	Demilitarised zones	Agencies MUST use demilitarised zones to house systems and information directly accessed externally.	Functional	Intersects With	DMZ Networks	NET-08.1	Mechanisms exist to monitor De-Militarized Zone (DMZ) network segments to separate untrusted networks from trusted networks.	5	
19.1.14.C.02	Demilitarised zones	Agencies SHOULD use demilitarised zones to house systems and information directly accessed externally.	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	
19.1.14.C.02	Demilitarised zones	Agencies SHOULD use demilitarised zones to house systems and information directly accessed externally.	Functional	Intersects With	DMZ Networks	NET-08.1	Mechanisms exist to monitor De-Militarized Zone (DMZ) network segments to separate untrusted networks from trusted networks.	5	
19.1.15.C.01	Risk assessment	Agencies MUST perform a risk assessment on gateways and their configuration prior to their implementation.	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	
19.1.16.C.01	Risk transfer	All domain and system owners connected through a gateway MUST understand and accept the residual security risk of the gateway and from any connected domains including those via a cascaded connection.	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	
19.1.16.C.02	Risk transfer	Agencies SHOULD annually review the security architecture of the gateway and risks of all connected domains including those via a cascaded connection.	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	
19.1.17.C.01	Information stakeholders and Shared Ownership	Once connectivity is established, domain owners MUST be considered information stakeholders for all connected 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	
19.1.17.C.02	Information stakeholders and Shared Ownership	Once connectivity is established, domain owners SHOULD be considered information stakeholders for all connected 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	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
19.1.18.C.01	System user training	All system users MUST be trained on the secure use and security risks of the gateways before being granted access.	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	
19.1.18.C.02	System user training	All system users SHOULD be trained in the secure use and security risks of the gateways before being granted access.	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	
19.1.19.C.01	Administration of gateways	Agencies MUST limit access to gateway administration functions.	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	
19.1.19.C.02	Administration of gateways	Agencies MUST ensure that system administrators are formally trained to manage gateways by qualified trainers.	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	
19.1.19.C.03	Administration of gateways	Agencies MUST ensure that all system administrators of gateways that process NZEO information meet the nationality requirements for these endorsements.	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	
19.1.19.C.04	Administration of gateways	Agencies MUST separate roles for the administration of gateways (e.g. separate network and security policy configuration roles).	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	
19.1.19.C.05	Administration of gateways	Agencies SHOULD separate roles for the administration of gateways (e.g. separate network and security policy configuration roles).	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	
19.1.20.C.01	System user authentication	Agencies MUST authenticate system users to all classified networks accessed through 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	
19.1.20.C.02	System user authentication	Agencies MUST ensure that only authenticated and authorised system users can use the gateway.	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	
19.1.20.C.03	System user authentication	Agencies SHOULD use multi-factor authentication for access to networks and 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	
19.1.21.C.01	IT equipment authentication	Agencies SHOULD authenticate any IT equipment that connects to networks accessed through 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	
19.1.22.C.01	Configuration control	Agencies MUST undertake a risk assessment and update the SRMP before changes are implemented.	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	
19.1.22.C.02	Configuration control	Agencies MUST document any changes to gateways in accordance with the agency's Change Management Policy.	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	
19.1.22.C.03	Configuration control	Agencies SHOULD undertake a risk assessment and update the SRMP before changes are implemented.	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	
19.1.23.C.01	Testing of gateways	Agencies SHOULD ensure that testing of security measures is performed at random intervals no more than six months apart.	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	
19.2.15.C.01	Gateway classification	For the purposes of this Manual, the CDS MUST be classified at the highest classification of connected domains.	Functional	Intersects With	Cross Domain Solution (CDS)	NET-02.3	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	5	
19.2.16.C.01	Allowable gateways	Agencies connecting a TOP SECRET, SECRET OR CONFIDENTIAL network to any other network MUST implement a CDS.	Functional	Intersects With	Cross Domain Solution (CDS)	NET-02.3	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	5	
19.2.16.C.02	Allowable gateways	Agencies MUST NOT implement a gateway permitting data to flow directly from: a TOP SECRET network to any network below SECRET; a SECRET network to an UNCLASSIFIED network; or a CONFIDENTIAL network to an UNCLASSIFIED network.	Functional	Intersects With	Cross Domain Solution (CDS)	NET-02.3	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	5	
19.2.17.C.01	Implementing Cross Domain Solutions	When designing and deploying a CDS, agencies MUST consult with the GCSB and comply with all directions provided.	Functional	Intersects With	Cross Domain Solution (CDS)	NET-02.3	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	5	
19.2.17.C.02	Implementing Cross Domain Solutions	Agencies connecting a typical gateway and a CDS to a common network MUST consult the GCSB on the impact to the security of the CDS and comply with all directions provided.	Functional	Intersects With	Cross Domain Solution (CDS)	NET-02.3	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	5	
19.2.18.C.01	Separation of data flows	Agencies MUST ensure that all bi-directional gateways between TOP SECRET and SECRET networks, SECRET and less classified networks, and CONFIDENTIAL and less classified networks, have separate upward and downward paths which use a diode and physically separate infrastructure for each path.	Functional	Intersects With	Cross Domain Solution (CDS)	NET-02.3	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	5	
19.2.19.C.01	Trusted sources	Trusted sources MUST be: a strictly limited list derived from business requirements and the result of a security risk assessment; where necessary an appropriate security clearance is held; and approved by the Accreditation Authority.	Functional	Intersects With	Cross Domain Solution (CDS)	NET-02.3	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	5	
19.2.19.C.02	Trusted sources	Trusted sources MUST authorise all data to be exported from a security domain.	Functional	Intersects With	Cross Domain Solution (CDS)	NET-02.3	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	5	
19.2.20.C.01	Operation of the Cross Domain Solution	All data exported from a security domain MUST be logged.	Functional	Intersects With	Cross Domain Solution (CDS)	NET-02.3	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	5	
19.3.8.C.01	Firewall assurance levels	All gateways MUST contain a firewall in both physical and virtual environments.	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	
19.3.8.C.02	Firewall assurance levels	Agencies MUST check the evaluation has examined the security enforcing functions by reviewing the target of evaluation/security target and other testing documentation.	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	
19.3.8.C.03	Firewall assurance levels	Agencies MUST use devices as shown in the following table for their gateway when connecting two networks of different classifications or two networks of the same classification but of different security domains. Your network Their network You require They require RESTRICTED and below UNCLASSIFIED EAL4 firewall N/A RESTRICTED EAL2 or PP firewall EAL2 or PP firewall CONFIDENTIAL EAL2 or PP firewall EAL4 firewall SECRET EAL2 or PP firewall EAL4 firewall TOP SECRET EAL2 or PP firewall Consultation with GCSB CONFIDENTIAL UNCLASSIFIED Consultation with GCSB N/A RESTRICTED	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	
19.3.8.C.04	Firewall assurance levels	The requirement to implement a firewall as part of gateway architecture MUST be met separately and independently by both parties (gateways) in both physical and virtual environments. Shared equipment DOES NOT satisfy the requirements of this control.	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	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
19.3.9.C.01	Firewall assurance levels for NZEO networks	Agencies MUST use a firewall of at least an EAL4 assurance level between an NZEO network and a foreign network in addition to the minimum assurance levels for firewalls between networks of different classifications or 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	
19.3.9.C.02	Firewall assurance levels for NZEO networks	In all other circumstances the table at 19.3.8.C.03 MUST apply.	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	
19.3.9.C.03	Firewall assurance levels for NZEO networks	Agencies SHOULD use a firewall of at least an EAL2 assurance level or a Protection Profile between an NZEO network and another New Zealand controlled network within a single security domain.	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	
19.4.4.C.01	Diode assurance levels	Agencies MUST use devices as shown in the following table for controlling the data flow of one-way gateways between networks of different classifications. High network Low network You require RESTRICTED UNCLASSIFIED EAL2 or PP diode RESTRICTED EAL2 or PP diode CONFIDENTIAL UNCLASSIFIED high assurance diode RESTRICTED high assurance diode CONFIDENTIAL high assurance diode SECRET UNCLASSIFIED high assurance diode RESTRICTED high assurance diode CONFIDENTIAL high assurance diode SECRET high assurance diode	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	
19.4.5.C.01	Diode assurance levels for NZEO networks	Agencies MUST use a diode of at least an EAL4 assurance level between an NZEO network and a foreign network in addition to the minimum assurance levels for diodes between networks of different classifications.	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	
19.4.5.C.02	Diode assurance levels for NZEO networks	In all other circumstances the table at 19.4.4.C.01 MUST apply.	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	
19.4.5.C.03	Diode assurance levels for NZEO networks	Agencies SHOULD use a diode of at least an EAL2 assurance level or a Protection Profile between an NZEO network and another New Zealand controlled network within a single security domain.	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	
19.4.6.C.01	Volume Checking	Agencies deploying a diode to control data flow within one-way gateways SHOULD monitor the volume of the data being transferred.	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	
19.5.24.C.01	Risk Assessment	Agencies intending to adopt VoIP or UC technologies or services MUST conduct a comprehensive risk assessment before implementation or adoption.	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	
19.5.24.C.02	Risk Assessment	Agencies intending to adopt VoIP or UC technologies or services MUST consider the risks to the availability of systems and information in their design of VoIP and UC systems architecture, fault tolerance, fail over and supporting controls and governance processes.	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	
19.5.24.C.03	Risk Assessment	Agencies MUST ensure risks for any VoIP or UC service adopted are understood and formally accepted by the agency's Accreditation Authority as part of the Certification and Accreditation process (See Chapter 4 - System Certification and Accreditation).	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	
19.5.24.C.04	Risk Assessment	Agencies intending to adopt VoIP or UC technologies or services MUST determine where the responsibility (agency or VoIP and UC service provider) for implementing, managing and maintaining controls lies in accordance with agreed trust boundaries.	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	
19.5.24.C.05	Risk Assessment	Any contracts for the provision of VoIP or UC services MUST include service level, availability, recoverability and restoration provisions as formally determined by business requirements.	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	
19.5.24.C.06	Risk Assessment	Agencies MUST ensure contracts with VoIP or UC service providers include provisions to manage risks associated with the merger, acquisition, liquidation or bankruptcy of the service provider and any subsequent termination of VoIP or UC 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	
19.5.24.C.07	Risk Assessment	Agencies procuring or using VoIP or UC services to be used by multiple agencies MUST ensure all interested parties formally agree to the risks, controls and any residual risks of such VoIP and UC services. The lead agency normally has this responsibility (see Chapter 2 - Information Security services within Government and Chapter 4 - System Certification and Accreditation).	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	
19.5.24.C.08	Risk Assessment	Agencies SHOULD consider the use of assessment tools, such as penetration testing, when undertaking the risk assessment.	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	
19.5.25.C.01	Non-Agency Networks	Agencies MUST follow the gateway requirements described in Chapter 19 - Gateway Security.	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	
19.5.26.C.01	Security Architecture and Configuration	Agencies intending to adopt VoIP or UC technologies or services MUST determine trust boundaries before implementation.	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	
19.5.26.C.02	Security Architecture and Configuration	Updates to the SBC and related devices MUST be verified by the administrator to ensure they are obtained from a trusted source and are unaltered.	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	
19.5.26.C.03	Security Architecture and Configuration	Agencies MUST include defence mechanisms for the Common VoIP and UC Security Risks and Threats described in 19.5.10.	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	
19.5.26.C.04	Security Architecture and Configuration	Agency networks MUST ensure the SBC includes a topology hiding capability.	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	
19.5.26.C.05	Security Architecture and Configuration	Agency networks MUST consider the use of call diversity and call failover 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	
19.5.26.C.06	Security Architecture and Configuration	In a virtualised environment, agencies MUST ensure any data contained in a protected resource is deleted or not available when the virtual resource is reallocated.	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	
19.5.26.C.07	Security Architecture and Configuration	Agencies SHOULD conduct a traffic analysis to ensure the agency's network and architecture is capable of supporting all VoIP, media and UC traffic. The traffic analysis SHOULD also determine any high availability requirements.	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	
19.5.26.C.08	Security Architecture and Configuration	Agencies SHOULD design a security and gateway architecture that segregates UC and normal data traffic. Firewall requirements (Section 19.3 - Firewalls) continue to apply to data traffic.	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	
19.5.26.C.09	Security Architecture and Configuration	In a virtualised environment, agencies SHOULD create separate virtual LANs for data traffic and UC traffic.	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	
19.5.26.C.10	Security Architecture and Configuration	In a non-virtualised environment, agencies SHOULD create separate LANs for data traffic and UC traffic.	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	
19.5.26.C.11	Security Architecture and Configuration	Agency networks SHOULD use encryption internally on VoIP and unified communications traffic.	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	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
19.5.26.C.12	Security Architecture and Configuration	Agency networks SHOULD ensure intrusion prevention systems and firewalls are VoIP-aware.	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	
19.5.27.C.01	Access Control	Any shared facilities MUST be clearly identifiable both physically and logically.	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	
19.5.27.C.02	Access Control	Agencies MUST provide a protected communication channel for administrators, and authorised systems personnel. Such communication MUST be logged.	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	
19.5.27.C.03	Access Control	Agencies MUST ensure administrative access to the SBC is available only through a trusted LAN and secure communication path.	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	
19.5.27.C.04	Access Control	Access control and password requirements SHOULD apply to VoIP and UC networks in all cases where individual access is granted.	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	
19.5.27.C.05	Access Control	In special cases where individual UserIDs and Passwords are impractical, a risk assessment SHOULD be completed and compensating controls applied.	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	
19.5.27.C.06	Access Control	Event logs covering all VoIP and UC services SHOULD be maintained in accordance with the requirements of the NZISM. See sections 16.6 - Event Logging and Auditing and 13.1.12 - Archiving.	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	
19.5.28.C.01	Incident Handling and Management	Agencies MUST include incident handling and management services in contracts with service providers.	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	
19.5.28.C.02	Incident Handling and Management	Agencies MUST develop and implement incident identification and management processes in accordance with this manual (See Chapter 6 - Information Security Monitoring, Chapter 7 - Information Security Incidents, Chapter 9 - Personnel Security and Chapter 16 - Access control and passwords).	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	
19.5.28.C.03	Incident Handling and Management	Agencies SHOULD implement fraud detection monitoring to identify suspicious activity and provide alerting so that remedial action can be taken.	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	
19.5.28.C.04	Incident Handling and Management	Agencies SHOULD regularly review call detail records for patterns of service theft.	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	
19.5.28.C.05	Incident Handling and Management	Agencies SHOULD consider the use of allow and deny listing to manage fraudulent calls to known fraudulent call destinations.	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	
19.5.28.C.06	Incident Handling and Management	Agencies SHOULD consider the use of call rate limiting as a fraud mitigation measure.	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	
19.5.28.C.07	Incident Handling and Management	Agencies SHOULD consider the use of call redirection to manage blocked calls.	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	
19.5.29.C.01	User Awareness and Training	Agencies MUST develop and implement user awareness and training programmes to support and enable safe use of VoIP and UC services (See Section 9.1 - Information Security Awareness and Training).	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	
20.1.20.C.01	Applicability	The use of cloud services and infrastructures for systems and data classified CONFIDENTIAL, SECRET or TOP SECRET MUST be approved by the GCSB.	Functional	Subset Of	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	10	
20.1.20.C.02	Applicability	Agencies intending to adopt cloud technologies or services MUST ensure cloud service providers apply the controls specified in this manual to any systems hosting, processing or storing agency data and systems.	Functional	Subset Of	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	10	
20.1.20.C.03	Applicability	Agencies MUST NOT use public, hybrid (incorporating a public element), or other external cloud services for systems and data classified CONFIDENTIAL, SECRET or TOP SECRET.	Functional	Subset Of	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	10	
20.1.20.C.04	Applicability	Agencies MUST NOT use public or hybrid (incorporating a public element) cloud services to host, process, store or transmit NZEO endorsed information.	Functional	Subset Of	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	10	
20.1.20.C.05	Applicability	Agencies intending to adopt cloud technologies or services SHOULD obtain formal assurance cloud service providers will apply the controls specified in this manual to any cloud service hosting, processing or storing agency data and systems.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	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	
20.1.21.C.01	Risk Assessment	Agencies intending to adopt cloud technologies or services MUST conduct a risk assessment before implementation or adoption.	Functional	Intersects With	Assessments	IAO-02	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	
20.1.21.C.02	Risk Assessment	Agencies intending to adopt cloud technologies or services MUST determine trust boundaries before implementation.	Functional	Intersects With	Assessment Boundaries	IAO-01.1	Mechanisms exist to establish the scope of assessments by defining the assessment boundary, according to people, processes and technology that directly or indirectly impact the confidentiality, integrity, availability and safety of the Technology Assets, Applications, Services and/or Data (TAASD) under review.	5	
20.1.21.C.03	Risk Assessment	Agencies intending to adopt cloud technologies or services MUST determine where the responsibility (agency or cloud service provider) for implementing, managing and maintaining controls lies in accordance with agreed trust boundaries.	Functional	Intersects With	Customer Responsibility Matrix (CRM)	CLD-06.1	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.	5	
20.1.21.C.04	Risk Assessment	Agencies MUST ensure cloud risks for any cloud service adopted are understood and formally accepted by the Agency Head or Chief Executive (or their formal delegate) and the agency's Accreditation Authority.	Functional	Intersects With	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	5	
20.1.21.C.05	Risk Assessment	Agencies MUST consult with the GCDO to ensure the strategic and other cloud risks are comprehensively assessed.	Functional	No Relationship	N/A	N/A	N/A	0	
20.1.21.C.06	Risk Assessment	Agencies procuring or using cloud services to be used by multiple agencies MUST ensure all interested parties formally agree the risks, controls and any residual risks of such cloud services.	Functional	No Relationship	N/A	N/A	N/A	0	
20.1.21.C.07	Risk Assessment	Agencies using cloud services MUST ensure they have conducted a documented risk assessment, accepted any residual risks, and followed the endorsement procedure required by the GCDO.	Functional	Intersects With	Assessments	IAO-02	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	
20.1.22.C.01	Offshore Services	Agencies using cloud services hosted offshore MUST ensure jurisdictional, sovereignty and privacy risks are fully considered and formally accepted by the Agency Head or Chief Executive and the agency's Accreditation Authority.	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	CLD-09	Mechanisms exist to control the location of cloud processing/storage based on business requirements that includes statutory, regulatory and contractual obligations.	5	
20.1.22.C.01	Offshore Services	Agencies using cloud services hosted offshore MUST ensure jurisdictional, sovereignty and privacy risks are fully considered and formally accepted by the Agency Head or Chief Executive and the agency's Accreditation Authority.	Functional	Intersects With	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	5	
20.1.22.C.02	Offshore Services	Agencies using cloud services hosted offshore MUST ensure that the agency retains ownership of its information in any contract with the cloud service provider.	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	CLD-09	Mechanisms exist to control the location of cloud processing/storage based on business requirements that includes statutory, regulatory and contractual obligations.	5	
20.1.22.C.03	Offshore Services	Agencies using cloud services hosted offshore and connected to All-of-Government systems MUST ensure they have conducted a risk assessment, accepted any residual risks, and followed the endorsement procedure required by the GCDO.	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	CLD-09	Mechanisms exist to control the location of cloud processing/storage based on business requirements that includes statutory, regulatory and contractual obligations.	5	
20.1.22.C.03	Offshore Services	Agencies using cloud services hosted offshore and connected to All-of-Government systems MUST ensure they have conducted a risk assessment, accepted any residual risks, and followed the endorsement procedure required by the GCDO.	Functional	Intersects With	Assessments	IAO-02	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	
20.1.22.C.03	Offshore Services	Agencies using cloud services hosted offshore and connected to All-of-Government systems MUST ensure they have conducted a risk assessment, accepted any residual risks, and followed the endorsement procedure required by the GCDO.	Functional	Intersects With	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
20.1.22.C.04	Offshore Services	Agencies MUST NOT use cloud services hosted offshore for information or systems classified CONFIDENTIAL, SECRET or TOP SECRET.	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	CLD-09	Mechanisms exist to control the location of cloud processing/storage based on business requirements that includes statutory, regulatory and contractual obligations.	5	
20.1.22.C.05	Offshore Services	Agencies MUST NOT use cloud services hosted offshore for information with an NZEO endorsement.	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	CLD-09	Mechanisms exist to control the location of cloud processing/storage based on business requirements that includes statutory, regulatory and contractual obligations.	5	
20.1.22.C.05	Offshore Services	Agencies MUST NOT use cloud services hosted offshore for information with an NZEO endorsement.	Functional	Intersects With	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	5	
20.1.22.C.06	Offshore Services	Agencies SHOULD NOT use cloud services hosted offshore unless: privacy, information sensitivity and information value has been fully assessed by the agency; a comprehensive risk assessment is undertaken by the agency; controls to manage identified risks have been specified by the agency; and the cloud service provider is able to provide adequate assurance that these controls have been properly implemented before the agency uses the cloud service.	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	CLD-09	Mechanisms exist to control the location of cloud processing/storage based on business requirements that includes statutory, regulatory and contractual obligations.	5	
20.1.23.C.01	System Availability	Agencies intending to adopt cloud technologies or services MUST consider the risks to the availability of systems and information in their design of cloud systems architectures and supporting controls and governance processes.	Functional	Intersects With	Assessments	IAO-02	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	
20.1.23.C.02	System Availability	Any contracts for the provision of cloud services MUST include service level, availability, recoverability and restoration provisions.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	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	
20.1.23.C.03	System Availability	Agencies MUST ensure contracts with cloud service providers include provisions to manage risks associated with the merger, acquisition, liquidation or bankruptcy of the service provider and any subsequent termination of cloud services.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	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	
20.1.24.C.01	Unauthorised Access	Agencies intending to adopt cloud technologies or services SHOULD ensure cloud service providers apply the physical, virtual and access controls specified in this manual for agency systems and data protection.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	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	
20.1.24.C.02	Unauthorised Access	Agencies intending to adopt cloud technologies or services SHOULD apply separation and access controls to protect data and systems where support is provided by offshore technical staff.	Functional	Intersects With	Cloud Security Architecture	CLD-02	Mechanisms exist to ensure the cloud security architecture supports the organization's technology strategy to securely design, configure and maintain cloud employments.	5	
20.1.24.C.03	Unauthorised Access	Agencies intending to adopt cloud technologies or services SHOULD apply controls to detect and prevent unauthorised data transfers and multiple or large scale data transfers to offshore locations and entities.	Functional	Intersects With	Cloud Security Architecture	CLD-02	Mechanisms exist to ensure the cloud security architecture supports the organization's technology strategy to securely design, configure and maintain cloud employments.	5	
20.1.24.C.04	Unauthorised Access	Agencies intending to adopt cloud technologies or services SHOULD consider the use of encryption for data in transit and at rest.	Functional	Intersects With	Cloud Security Architecture	CLD-02	Mechanisms exist to ensure the cloud security architecture supports the organization's technology strategy to securely design, configure and maintain cloud employments.	5	
20.1.25.C.01	Incident Handling and Management	Agencies MUST include incident handling and management services in contracts with cloud service providers.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	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	
20.1.25.C.02	Incident Handling and Management	Agencies MUST develop and implement incident identification and management processes in accordance with this manual (See Chapter 6 - Information Security Monitoring, Chapter 7 - Information Security Incidents, Chapter 9 - Personnel Security and Chapter 16 - Access Control).	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
20.1.26.C.01	Backup, Recovery Archiving and Data Remanence	Agencies MUST develop and implement a backup, recovery and archiving plan and supporting procedures (See Section 6.4 - Business Continuity and Disaster Recovery).	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
20.1.26.C.02	Backup, Recovery Archiving and Data Remanence	Agencies MUST include a data purge or secure delete process in any cloud service contracts.	Functional	Intersects With	Cloud Infrastructure Offboarding	CLD-01.2	Mechanisms exist to ensure cloud services are decommissioned so that data is securely transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	
20.1.26.C.03	Backup, Recovery Archiving and Data Remanence	Any data purge or secure delete process in any cloud service contracts MUST be independently verifiable.	Functional	Intersects With	Cloud Infrastructure Offboarding	CLD-01.2	Mechanisms exist to ensure cloud services are decommissioned so that data is securely transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	
20.1.27.C.01	User Awareness and Training	Agencies MUST develop and implement user awareness and training programmes to support and enable safe use of cloud services (See Section 9.1 - Information Security Awareness and Training).	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	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	
20.2.12.C.01	Functional segregation between servers	Virtualisation technology MUST NOT be used for functional segregation between servers of different classifications.	Functional	Intersects With	Cloud Security Architecture	CLD-02	Mechanisms exist to ensure the cloud security architecture supports the organization's technology strategy to securely design, configure and maintain cloud employments.	5	
20.2.12.C.01	Functional segregation between servers	Virtualisation technology MUST NOT be used for functional segregation between servers of different classifications.	Functional	Intersects With	Cross Domain Solution (CDS)	NET-02.3	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	5	
20.2.12.C.01	Functional segregation between servers	Virtualisation technology MUST NOT be used for functional segregation between servers of different classifications.	Functional	Intersects With	Virtualization Techniques	SEA-13.1	Mechanisms exist to utilize virtualization techniques to support the employment of a diversity of operating systems and applications.	5	
20.2.12.C.02	Functional segregation between servers	Virtualisation technology MUST NOT be used for functional segregation between servers in different security domains at the same classification.	Functional	Intersects With	Cloud Security Architecture	CLD-02	Mechanisms exist to ensure the cloud security architecture supports the organization's technology strategy to securely design, configure and maintain cloud employments.	5	
20.2.12.C.02	Functional segregation between servers	Virtualisation technology MUST NOT be used for functional segregation between servers in different security domains at the same classification.	Functional	Intersects With	Cross Domain Solution (CDS)	NET-02.3	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	5	
20.2.12.C.02	Functional segregation between servers	Virtualisation technology MUST NOT be used for functional segregation between servers in different security domains at the same classification.	Functional	Intersects With	Virtualization Techniques	SEA-13.1	Mechanisms exist to utilize virtualization techniques to support the employment of a diversity of operating systems and applications.	5	
20.2.12.C.03	Functional segregation between servers	Agencies SHOULD ensure that functional segregation between servers is achieved by: physically, using single dedicated machines for each function; or using virtualisation technology to create separate virtual machines for each function within the same security domain.	Functional	Intersects With	Virtualization Techniques	SEA-13.1	Mechanisms exist to utilize virtualization techniques to support the employment of a diversity of operating systems and applications.	5	
20.2.12.C.04	Functional segregation between servers	Virtualisation technology SHOULD NOT be used for functional segregation between servers in different security domains at the same classification.	Functional	Intersects With	Virtualization Techniques	SEA-13.1	Mechanisms exist to utilize virtualization techniques to support the employment of a diversity of operating systems and applications.	5	
20.2.13.C.01	Risk Management	Agencies MUST undertake a virtualisation specific risk assessment in order to identify risks, related risk treatments and controls.	Functional	Intersects With	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; (11) Artificial Intelligence and Autonomous Technologies (AAT); and/or	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
20.2.13.C.02	Risk Management	Agencies SHOULD undertake a virtualisation specific risk assessment in order to identify risks and related risk treatments.	Functional	Intersects With	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; (11) Artificial Intelligence and Autonomous Technologies (AAT); and/or	5	
20.2.14.C.01	Systems Architecture	Agencies MUST architect virtualised systems and environments to enforce the principles of separation and segregation of key elements of the system using trust zones or security domains.	Functional	Intersects With	Secure Engineering Principles	SEA-01	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	
20.2.14.C.01	Systems Architecture	Agencies MUST architect virtualised systems and environments to enforce the principles of separation and segregation of key elements of the system using trust zones or security domains.	Functional	Intersects With	Virtualization Techniques	SEA-13.1	Mechanisms exist to utilize virtualization techniques to support the employment of a diversity of operating systems and applications.	5	
20.2.14.C.02	Systems Architecture	Agencies MUST NOT permit the sharing of files or other operating system components between host and guest operating systems.	Functional	Intersects With	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	5	
20.2.14.C.03	Systems Architecture	Agencies SHOULD architect virtualised systems and environments to enforce the principles of separation and segregation of key elements of the system using trust zones.	Functional	Intersects With	Secure Engineering Principles	SEA-01	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	
20.2.14.C.03	Systems Architecture	Agencies SHOULD architect virtualised systems and environments to enforce the principles of separation and segregation of key elements of the system using trust zones.	Functional	Intersects With	Virtualization Techniques	SEA-13.1	Mechanisms exist to utilize virtualization techniques to support the employment of a diversity of operating systems and applications.	5	
20.2.14.C.04	Systems Architecture	Agencies SHOULD design virtualised systems and environments to enable functional segregation within a security domain.	Functional	Intersects With	Cross Domain Solution (CDS)	NET-02.3	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	5	
20.2.14.C.04	Systems Architecture	Agencies SHOULD design virtualised systems and environments to enable functional segregation within a security domain.	Functional	Intersects With	Virtualization Techniques	SEA-13.1	Mechanisms exist to utilize virtualization techniques to support the employment of a diversity of operating systems and applications.	5	
20.2.14.C.05	Systems Architecture	Agencies SHOULD harden the host operating systems following an agency or other approved hardening guide.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
20.2.14.C.06	Systems Architecture	Agencies SHOULD separate production from test or development virtual environments.	Functional	Intersects With	Separation of Development, Testing and Operational Environments	TDA-08	Mechanisms exist to manage separate development, testing and operational environments to reduce the risks of unauthorized access or changes to the operational environment and to ensure no impact to production Technology Assets, Applications and/or Services (TAAS).	5	
20.2.14.C.07	Systems Architecture	Agencies SHOULD NOT permit the sharing of files or other operating system components between host and guest operating systems.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
20.2.14.C.07	Systems Architecture	Agencies SHOULD NOT permit the sharing of files or other operating system components between host and guest operating systems.	Functional	Intersects With	Virtualization Techniques	SEA-13.1	Mechanisms exist to utilize virtualization techniques to support the employment of a diversity of operating systems and applications.	5	
20.2.15.C.01	Systems Management	Agencies MUST ensure a VM migration policy and related SOPs are implemented.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
20.2.15.C.02	Systems Management	Agencies MUST implement controls to prohibit unauthorised VM migrations within a virtual environment or between physical environments.	Functional	Intersects With	Prohibition Of Changes	CHG-02.1	Mechanisms exist to prohibit unauthorized changes, unless organization-approved change requests are received.	5	
20.2.15.C.03	Systems Management	Agencies MUST implement controls to safely decommission VMs when no longer required, including elimination of images, snapshots, storage, backup, archives and any other residual data.	Functional	Intersects With	Decommissioning	AST-30	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are properly decommissioned so that data is properly transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	
20.2.15.C.04	Systems Management	Agencies SHOULD ensure a VM migration policy and related SOPs are implemented.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
20.2.15.C.04	Systems Management	Agencies SHOULD ensure a VM migration policy and related SOPs are implemented.	Functional	Intersects With	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	8	
20.2.15.C.05	Systems Management	Agencies SHOULD implement controls to prohibit unauthorised VM migrations within a virtual environment or between physical environments.	Functional	Intersects With	Prohibition Of Changes	CHG-02.1	Mechanisms exist to prohibit unauthorized changes, unless organization-approved change requests are received.	5	
20.2.15.C.06	Systems Management	Agencies SHOULD implement controls to safely decommission VMs when no longer required.	Functional	Intersects With	Decommissioning	AST-30	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are properly decommissioned so that data is properly transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	
20.2.15.C.07	Systems Management	Agencies SHOULD implement security and operational management and monitoring tools which include the following minimum capabilities: Identify VMs when initiated; Validate integrity of files prior to installation; Scan new VMs for vulnerabilities and misconfigurations; Load only minimum operating system components and services; Set resource usage limits; Establish connections to peripherals only as required; Ensure host and guest time synchronisation; Detect snapshot rollbacks and scans after restores; Track asset migration; and Monitor the security posture of migrated assets.	Functional	Subset Of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
20.2.15.C.07	Systems Management	Agencies SHOULD implement security and operational management and monitoring tools which include the following minimum capabilities: Identify VMs when initiated; Validate integrity of files prior to installation; Scan new VMs for vulnerabilities and misconfigurations; Load only minimum operating system components and services; Set resource usage limits; Establish connections to peripherals only as required; Ensure host and guest time synchronisation; Detect snapshot rollbacks and scans after restores; Track asset migration; and Monitor the security posture of migrated assets.	Functional	Intersects With	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	5	
20.2.16.C.01	Authentication and Access	Agencies MUST maintain strong physical security and physical access controls.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
20.2.16.C.02	Authentication and Access	Agencies MUST maintain strong authentication and access controls.	Functional	Intersects With	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	5	
20.2.16.C.03	Authentication and Access	Agencies SHOULD maintain strong data validation checks.	Functional	Intersects With	Data Governance	GOV-10	Mechanisms exist to facilitate data governance to oversee the organization's policies, standards and procedures so that sensitive and/or regulated data is effectively managed and maintained in accordance with applicable statutory, regulatory and contractual obligations.	5	
20.3.9.C.01	Using VLANs	The principles of separation and segregation MUST be applied to the design and architecture of VLANs.	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
20.3.9.C.02	Using VLANs	Agencies MUST NOT use VLANs between classified networks and any other network of a lower classification.	Functional	Intersects With	Cross Domain Solution (CDS)	NET-02.3	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	5	
20.3.9.C.02	Using VLANs	Agencies MUST NOT use VLANs between classified networks and any other network of a lower classification.	Functional	Intersects With	Virtual Local Area Network (VLAN) Separation	NET-06.2	Mechanisms exist to enable Virtual Local Area Networks (VLANs) to limit the ability of devices on a network to directly communicate with other devices on the subnet and limit an attacker's ability to laterally move to compromise neighboring systems.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
20.3.9.C.03	Using VLANs	Agencies MUST NOT use VLANs between any classified network and any unclassified network.	Functional	Intersects With	Virtual Local Area Network (VLAN) Separation	NET-06.2	Mechanisms exist to enable Virtual Local Area Networks (VLANs) to limit the ability of devices on a network to directly communicate with other devices on the subnet and limit an attacker's ability to laterally move to compromise neighboring systems.	5	
20.3.9.C.04	Using VLANs	VLAN trunking MUST NOT be used on switches managing VLANs of differing security domains.	Functional	Intersects With	Cross Domain Solution (CDS)	NET-02.3	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	5	
20.3.9.C.04	Using VLANs	VLAN trunking MUST NOT be used on switches managing VLANs of differing security domains.	Functional	Intersects With	Virtual Local Area Network (VLAN) Separation	NET-06.2	Mechanisms exist to enable Virtual Local Area Networks (VLANs) to limit the ability of devices on a network to directly communicate with other devices on the subnet and limit an attacker's ability to laterally move to compromise neighboring systems.	5	
20.3.10.C.01	Configuration and administration	Administrative access MUST be permitted only from the most trusted network.	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
20.3.11.C.01	Disabling unused ports	Unused ports on the switches MUST be disabled.	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
20.3.11.C.02	Disabling unused ports	Unused ports on the switches SHOULD be disabled.	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
21.1.6.C.01	User responsibilities	Agencies MUST establish a policy and train staff in the processes for data transfers between systems and the authorisations required before transfers can take place.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
21.1.6.C.01	User responsibilities	Agencies MUST establish a policy and train staff in the processes for data transfers between systems and the authorisations required before transfers can take place.	Functional	Intersects With	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive and/or regulated data is formally trained in data handling requirements.	8	
21.1.6.C.02	User responsibilities	Agencies MUST ensure that system users transferring data to and from a system are held accountable for the data they transfer.	Functional	Intersects With	Terms of Employment	HRS-05	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	
21.1.7.C.01	Data transfer processes and procedures	Agencies MUST ensure that data transfers are performed in accordance with processes and procedures approved by the Accreditation Authority.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
21.1.7.C.02	Data transfer processes and procedures	Agencies SHOULD ensure that data transfers are performed in accordance with processes and procedures approved by the Accreditation Authority.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
21.1.8.C.01	Data transfer authorisation	Agencies MUST ensure that all data transferred to a system of a lesser classification or a less secure system, is approved by a trusted source.	Functional	Intersects With	Cross Domain Solution (CDS)	NET-02.3	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	5	
21.1.9.C.01	Trusted sources	Trusted sources MUST be: a strictly limited list derived from business requirements and the result of a security risk assessment; where necessary an appropriate security clearance is held; and approved by the Accreditation Authority.	Functional	No Relationship	N/A	N/A	N/A	0	
21.1.10.C.01	Import of data	Agencies importing data to a system MUST ensure that the data is scanned for malicious and active content.	Functional	Subset Of	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	10	
21.1.10.C.02	Import of data	Agencies importing data to a system MUST implement the following controls: scanning for malicious and active content; data format checks; identify unexpected attachments or embedded objects; log each event; and monitoring to detect overuse/unusual usage patterns.	Functional	Subset Of	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	10	
21.1.11.C.01	Export of highly formatted textual data	When agencies export formatted textual data with no free text fields and all fields have a predefined set of permitted formats and data values, agencies MUST implement the following controls: protective marking checks; data validation and format checks; size limits; keyword checks; identify unexpected attachments or embedded objects; log each event; and monitoring to detect overuse/unusual usage patterns.	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
21.1.11.C.01	Export of highly formatted textual data	When agencies export formatted textual data with no free text fields and all fields have a predefined set of permitted formats and data values, agencies MUST implement the following controls: protective marking checks; data validation and format checks; size limits; keyword checks; identify unexpected attachments or embedded objects; log each event; and monitoring to detect overuse/unusual usage patterns.	Functional	Subset Of	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	10	
21.1.12.C.01	Export of other data	When agencies export data, other than highly formatted textual data, agencies MUST implement the following controls: protective marking checks; data validation and format checks; limitations on data types; size limits; keyword checks; identify unexpected attachments or embedded objects; log each event; and monitoring to detect overuse/unusual usage patterns.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
21.1.12.C.01	Export of other data	When agencies export data, other than highly formatted textual data, agencies MUST implement the following controls: protective marking checks; data validation and format checks; limitations on data types; size limits; keyword checks; identify unexpected attachments or embedded objects; log each event; and monitoring to detect overuse/unusual usage patterns.	Functional	Subset Of	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	10	
21.1.12.C.01	Export of other data	When agencies export data, other than highly formatted textual data, agencies MUST implement the following controls: protective marking checks; data validation and format checks; limitations on data types; size limits; keyword checks; identify unexpected attachments or embedded objects; log each event; and monitoring to detect overuse/unusual usage patterns.	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	
21.1.13.C.01	Preventing export of NZEO data to foreign systems	Agencies MUST: ensure that keyword searches are performed on all textual data; ensure that any identified data is quarantined until reviewed and approved for release by a trusted source other than the originator; and develop procedures to prevent NZEO information in both textual and non-textual formats from being exported.	Functional	Intersects With	Full Device & Container-Based Encryption	MDM-03	Cryptographic mechanisms exist to protect the confidentiality and integrity of information on mobile devices through full-device or container encryption.	5	
21.2.3.C.01	User responsibilities	Users transferring data to and from a system MUST be held accountable for the data they transfer.	Functional	Intersects With	Terms of Employment	HRS-05	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	
21.2.4.C.01	Data Transfer authorisation	All data transferred to a system of a lesser sensitivity or classification MUST be approved by a trusted source.	Functional	Intersects With	Work From Anywhere (WFA) - Telecommuting Security	NET-14.5	Mechanisms exist to define secure telecommuting practices and govern remote access to Technology Assets, Applications, Services and/or Data (TAASD) for remote workers.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
21.2.5.C.01	Trusted sources	Trusted sources MUST be: a strictly limited list derived from business requirements and the result of a security risk assessment; where necessary an appropriate security clearance is held; and approved by the Accreditation Authority.	Functional	Intersects With	Work From Anywhere (WFA) - Telecommuting Security	NET-14.5	Mechanisms exist to define secure telecommuting practices and govern remote access to Technology Assets, Applications, Services and/or Data (TAASD) for remote workers.	5	
21.2.6.C.01	Import of data through gateways	When agencies import data to a system through gateways, the data MUST be filtered by a product specifically designed for that purpose, including filtering malicious and active content.	Functional	Intersects With	Work From Anywhere (WFA) - Telecommuting Security	NET-14.5	Mechanisms exist to define secure telecommuting practices and govern remote access to Technology Assets, Applications, Services and/or Data (TAASD) for remote workers.	5	
21.2.6.C.02	Import of data through gateways	When agencies import data to a system through gateways, full or partial audits of the event logs MUST be performed at least monthly.	Functional	No Relationship	N/A	N/A	N/A	0	
21.2.6.C.03	Import of data through gateways	Agencies SHOULD convert data being imported at gateways into an alternative format before entering the network.	Functional	No Relationship	N/A	N/A	N/A	0	
21.2.7.C.01	Export of data through gateways	Agencies SHOULD restrict the export of data to a system of a lesser classification by filtering data using at least protective marking checks.	Functional	Intersects With	Work From Anywhere (WFA) - Telecommuting Security	NET-14.5	Mechanisms exist to define secure telecommuting practices and govern remote access to Technology Assets, Applications, Services and/or Data (TAASD) for remote workers.	5	
21.2.8.C.01	Export of highly formatted textual data through gateways	When the export of highly formatted textual data occurs through gateways agencies MUST implement: checks for protective markings; data filtering performed by a product specifically designed for that purpose; data range and data type checks; and full or partial audits of the event logs performed at least monthly.	Functional	No Relationship	N/A	N/A	N/A	0	
21.2.9.C.01	Export of other data through gateways	When agencies export data, other than highly formatted textual data, through gateways, agencies MUST implement data filtering performed by a product specifically designed for that purpose.	Functional	No Relationship	N/A	N/A	N/A	0	
21.2.9.C.02	Export of other data through gateways	When agencies do not perform audits of the complete data transfer logs at least monthly they MUST perform randomly timed audits of random subsets of the data transfer logs on a weekly basis.	Functional	No Relationship	N/A	N/A	N/A	0	
21.2.9.C.03	Export of other data through gateways	Where the classification cannot be determined automatically, a human trusted source SHOULD assess the classification of the data.	Functional	No Relationship	N/A	N/A	N/A	0	
21.2.9.C.04	Export of other data through gateways	When the export of other data occurs through gateways agencies SHOULD perform audits of the complete data transfer logs at least monthly.	Functional	No Relationship	N/A	N/A	N/A	0	
21.2.10.C.01	Preventing export of NZEO data to foreign systems	To prevent the export of NZEO data to foreign systems, agencies MUST implement NZEO data filtering performed by a product specifically designed or configured for that purpose.	Functional	No Relationship	N/A	N/A	N/A	0	
21.2.10.C.02	Preventing export of NZEO data to foreign systems	Agencies MUST undertake checks of protective markings and keywords before permitting data export.	Functional	No Relationship	N/A	N/A	N/A	0	
21.2.11.C.01	Requirement to sign exported data	A trusted source MUST sign the data to be exported if the data is to be communicated over a network to which untrusted personnel or systems have access.	Functional	No Relationship	N/A	N/A	N/A	0	
21.2.11.C.02	Requirement to sign exported data	Agencies MUST ensure that the gateway verifies authority to release prior to the release of the data to be exported.	Functional	No Relationship	N/A	N/A	N/A	0	
21.2.11.C.03	Requirement to sign exported data	Agencies SHOULD use a product evaluated to at least an EAL4 assurance level for the purpose of data signing and signature confirmation.	Functional	No Relationship	N/A	N/A	N/A	0	
21.3.4.C.01	Limiting transfers by file type	Agencies MUST strictly define and limit the types of files that can be transferred based on business requirements and the results of a security risk assessment.	Functional	No Relationship	N/A	N/A	N/A	0	
21.3.4.C.02	Limiting transfers by file type	Agencies SHOULD strictly define and limit the types of files that can be transferred based on business requirements and the results of a security risk assessment.	Functional	No Relationship	N/A	N/A	N/A	0	
21.3.5.C.01	Blocking active content	Agencies MUST block all executables and active content from entering a security domain.	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	
21.3.5.C.02	Blocking active content	Agencies SHOULD block all executables and active content from being communicated though 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	
21.3.6.C.01	Blocking suspicious data	Agencies MUST block, quarantine or drop any data identified by a data filter as suspicious until reviewed and approved for transfer by a trusted source other than the originator.	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	
21.3.7.C.01	Content validation	Agencies MUST perform validation on all data passing through a content filter, blocking content which fails the validation.	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
21.3.7.C.02	Content validation	Agencies SHOULD perform validation on all data passing through a content filter, blocking content which fails the validation.	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
21.3.8.C.01	Content conversion and transformation	Agencies SHOULD perform content conversion, file conversion or both for all ingress or egress data transiting a security domain boundary.	Functional	No Relationship	N/A	N/A	N/A	0	
21.3.9.C.01	Content sanitisation	Agencies SHOULD perform content and file sanitisation on suitable file types if content conversion or file conversion is not appropriate for data transiting a security domain boundary.	Functional	No Relationship	N/A	N/A	N/A	0	
21.3.10.C.01	Antivirus scans	Agencies SHOULD perform antivirus scans on all content using up-to-date engines and signatures, using multiple different scanning engines.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
21.3.11.C.01	Archive and container files	Agencies SHOULD extract the contents from archive and container files and subject the extracted files to content filter tests.	Functional	No Relationship	N/A	N/A	N/A	0	
21.3.11.C.02	Archive and container files	Agencies SHOULD perform controlled inspection of archive and container files to ensure that content filter performance and availability is not adversely affected.	Functional	No Relationship	N/A	N/A	N/A	0	
21.3.11.C.03	Archive and container files	Agencies SHOULD block files that cannot be inspected and generate an alert or notification.	Functional	No Relationship	N/A	N/A	N/A	0	
21.3.12.C.01	Allow listing permitted content	Agencies MUST create and enforce an allow list of permitted content types based on business requirements and the results of a security risk assessment.	Functional	No Relationship	N/A	N/A	N/A	0	
21.3.12.C.02	Allow listing permitted content	Agencies SHOULD create and enforce an allow list of permitted content types based on business requirements and the results of a security risk assessment.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5	
21.3.13.C.01	Data integrity	If data is signed, agencies MUST ensure that the signature is validated before the data is exported.	Functional	No Relationship	N/A	N/A	N/A	0	
21.3.13.C.02	Data integrity	Agencies SHOULD verify the integrity of content where applicable, and block the content if verification fails.	Functional	No Relationship	N/A	N/A	N/A	0	
21.3.14.C.01	Encrypted data	Agencies SHOULD decrypt and inspect all encrypted content, traffic and data to allow content filtering.	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
21.3.15.C.01	Monitoring data import and export	Agencies MUST use protective marking checks to restrict the export of data from each security domain, including through a gateway.	Functional	No Relationship	N/A	N/A	N/A	0	
21.3.15.C.02	Monitoring data import and export	When importing data to each security domain, including through a gateway, agencies MUST audit the complete data transfer logs at least monthly.	Functional	No Relationship	N/A	N/A	N/A	0	
21.3.16.C.01	Exception Handling	Agencies SHOULD create an exception handling process to deal with blocked or quarantined file types that may have a valid requirement to be transferred.	Functional	No Relationship	N/A	N/A	N/A	0	
21.4.3.C.01	Data labelling	Agencies MUST ensure that all classified information stored within a database is associated with an appropriate protective marking if the information: could be exported to a different system; or contains differing classifications or different handling requirements.	Functional	No Relationship	N/A	N/A	N/A	0	
21.4.3.C.02	Data labelling	Agencies MUST ensure that protective markings are applied with a level of granularity sufficient to clearly define the handling requirements for any classified information retrieved or exported from a database.	Functional	No Relationship	N/A	N/A	N/A	0	
21.4.3.C.03	Data labelling	Agencies SHOULD ensure that all classified information stored within a database is associated with an appropriate protective marking if the information: could be exported to a different system; or contains differing classifications or different handling requirements.	Functional	No Relationship	N/A	N/A	N/A	0	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
21.4.3.C.04	Data labelling	Agencies SHOULD ensure that protective markings are applied with a level of granularity sufficient to clearly define the handling requirements for any classified information retrieved or exported from a database.	Functional	No Relationship	N/A	N/A	N/A	0	
21.4.4.C.01	Database files	Agencies MUST protect database files from access that bypasses the databases normal access controls.	Functional	No Relationship	N/A	N/A	N/A	0	
21.4.4.C.02	Database files	Agencies SHOULD protect database files from access that bypass normal access controls.	Functional	No Relationship	N/A	N/A	N/A	0	
21.4.5.C.01	Accountability	Agencies MUST enable logging and auditing of system users actions.	Functional	No Relationship	N/A	N/A	N/A	0	
21.4.5.C.02	Accountability	Agencies SHOULD ensure that databases provide functionality to allow for auditing of system users actions.	Functional	No Relationship	N/A	N/A	N/A	0	
21.4.6.C.01	Search engines	If results from database queries cannot be appropriately filtered, agencies MUST ensure that all query results are appropriately sanitised to meet the minimum security clearances of system users.	Functional	No Relationship	N/A	N/A	N/A	0	
21.4.6.C.02	Search engines	Agencies SHOULD ensure that system users who do not have sufficient security clearances to view database contents cannot see or interrogate associated metadata in a list of results from a search engine query.	Functional	No Relationship	N/A	N/A	N/A	0	
22.1.10.C.01	Mobile devices usage policy	Agencies MUST develop a policy governing the use of mobile devices.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
22.1.10.C.01	Mobile devices usage policy	Agencies MUST develop a policy governing the use of mobile devices.	Functional	Intersects With	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	5	
22.1.10.C.02	Mobile devices usage policy	Agencies MUST NOT allow mobile devices to process or store TOP SECRET information unless explicitly approved by GCSB to do so.	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
22.1.10.C.03	Mobile devices usage policy	Agencies SHOULD implement a Mobile Device Management (MDM) solution.	Functional	Intersects With	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	5	
22.1.11.C.01	Personnel awareness	Agencies MUST advise personnel of the maximum permitted classifications for data and voice communications when using mobile devices.	Functional	Intersects With	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive and/or regulated data is formally trained in data handling requirements.	5	
22.1.11.C.02	Personnel awareness	Agencies SHOULD NOT use Paging Services, SMS or MMS for sensitive or classified communications.	Functional	No Relationship	N/A	N/A	N/A	0	
22.1.12.C.01	Non-agency owned and controlled mobile devices	Agencies MUST apply the full set of BYOD controls for devices NOT directly owned and controlled by the agency. These controls are detailed in Section 21.4 - BYOD.	Functional	Intersects With	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	5	
22.1.13.C.01	Agency owned mobile device storage encryption	Agencies unable to lower the storage and physical transfer requirements of a mobile device to an unclassified level through the use of encryption MUST physically store or transfer the device as a classified asset in accordance with the relevant handling instructions.	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
22.1.13.C.02	Agency owned mobile device storage encryption	Users MUST NOT store passwords, passphrases, PINs or other access codes for encryption on or with the mobile device on which data will be encrypted when the device is issued for normal operations.	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
22.1.13.C.03	Agency owned mobile device storage encryption	Agencies unable to lower the storage and physical transfer requirements of a mobile device to an unclassified level through the use of encryption SHOULD physically store or transfer the device as a classified asset in accordance with the relevant handling instructions.	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
22.1.13.C.04	Agency owned mobile device storage encryption	Agencies SHOULD encrypt classified information on all mobile devices using an Approved Cryptographic Algorithm.	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
22.1.13.C.05	Agency owned mobile device storage encryption	Pool or shared devices SHOULD be reissued with unique passwords, passphrases, PINs or other access codes for each separate issue or deployment.	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
22.1.14.C.01	Mobile device communications encryption	Agencies MUST use encryption on mobile devices communicating over public infrastructure, the Internet or non-agency controlled networks.	Functional	Intersects With	Full Device & Container-Based Encryption	MDM-03	Cryptographic mechanisms exist to protect the confidentiality and integrity of information on mobile devices through full-device or container encryption.	5	
22.1.14.C.02	Mobile device communications encryption	Agencies SHOULD use encryption for Official Information or any classified information on mobile devices communicating over public infrastructure, the Internet or non-agency controlled networks.	Functional	Intersects With	Full Device & Container-Based Encryption	MDM-03	Cryptographic mechanisms exist to protect the confidentiality and integrity of information on mobile devices through full-device or container encryption.	5	
22.1.15.C.01	Mobile device privacy filters	Agencies SHOULD apply privacy filters to the screens of mobile devices.	Functional	Intersects With	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	5	
22.1.16.C.01	Disabling Bluetooth functionality	Agencies MUST NOT enable Bluetooth functionality on mobile devices.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
22.1.16.C.02	Disabling Bluetooth functionality	Agencies SHOULD NOT enable Bluetooth functionality on mobile devices.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
22.1.17.C.01	Configuration control	Agency personnel MUST NOT disable security functions or security configurations on a mobile device once provisioned.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
22.1.17.C.02	Configuration control	Agencies SHOULD control the configuration of mobile devices in the same manner as devices in the agency's office environment.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
22.1.17.C.03	Configuration control	Agencies SHOULD prevent personnel from installing unauthorised applications on a mobile device once provisioned.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
22.1.18.C.01	Maintaining mobile device security	Agencies SHOULD ensure that mobile devices have security updates applied on a regular basis and are tested to ensure that the mobile devices are still secure.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	
22.1.18.C.02	Maintaining mobile device security	Agencies SHOULD conduct policy checks as mobile devices connect to agency systems.	Functional	Intersects With	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	5	
22.1.19.C.01	Connecting mobile devices to the Internet	Agencies MUST disable split tunnelling when using a VPN connection from a mobile device to connect to an agency network.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
22.1.19.C.02	Connecting mobile devices to the Internet	Agencies SHOULD NOT allow mobile devices to connect to the Internet except when temporarily connecting to facilitate the establishment of a VPN connection to an agency network.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
22.1.20.C.01	Emergency destruction	Agencies MUST develop an emergency destruction plan for mobile devices.	Functional	Subset Of	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	10	
22.1.20.C.02	Emergency destruction	If a cryptographic zeroise or sanitise function is provided for cryptographic keys on a mobile device it MUST be used as part of the emergency destruction procedures.	Functional	Subset Of	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	10	
22.1.20.C.03	Emergency destruction	Agencies SHOULD ensure personnel are trained in emergency destruction procedures and are familiar with the emergency destruction plan.	Functional	Subset Of	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	10	
22.1.21.C.01	Labelling	Agencies SHOULD use soft labelling for mobile devices when appropriate to reduce their attractiveness value.	Functional	Subset Of	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	10	
22.1.22.C.01	Unauthorised use of mobile devices	Agencies SHOULD develop a policy to manage the non-business or personal use of an agency owned device.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
22.1.22.C.01	Unauthorised use of mobile devices	Agencies SHOULD develop a policy to manage the non-business or personal use of an agency owned device.	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	CLD-09	Mechanisms exist to control the location of cloud processing/storage based on business requirements that includes statutory, regulatory and contractual obligations.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
22.1.22.C.02	Unauthorised use of mobile devices	Mobile devices SHOULD NOT be used other than by personnel specifically authorised by the agency.	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	CLD-09	Mechanisms exist to control the location of cloud processing/storage based on business requirements that includes statutory, regulatory and contractual obligations.	5	
22.2.4.C.01	Working outside the office	Agencies MUST NOT allow personnel to access or communicate classified information on mobile devices outside of secure areas unless there is a reduced chance of being overheard and having the screen of the device observed.	Functional	Intersects With	Work From Anywhere (WFA) - Telecommuting Security	NET-14.5	Mechanisms exist to define secure telecommuting practices and govern remote access to Technology Assets, Applications, Services and/or Data (TAASD) for remote workers.	5	
22.2.4.C.02	Working outside the office	Agencies allowing personnel to access or communicate classified information outside of the office SHOULD NOT allow personnel to do so in public locations (e.g. public transport, transit lounges, hotel lobbies and coffee shops).	Functional	Intersects With	Work From Anywhere (WFA) - Telecommuting Security	NET-14.5	Mechanisms exist to define secure telecommuting practices and govern remote access to Technology Assets, Applications, Services and/or Data (TAASD) for remote workers.	5	
22.2.5.C.01	Carrying mobile devices	Agencies MUST ensure mobile devices are carried in a secured state when not being actively used, by: power off; or power on but pass code enabled.	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
22.2.6.C.01	Using mobile devices	When in use mobile devices MUST be kept under continual direct supervision.	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
22.2.7.C.01	Travelling with mobile devices	When travelling with mobile devices and media, personnel MUST retain control over them at all times including by not placing them in checked-in luggage or leaving them unattended.	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
22.2.7.C.02	Travelling with mobile devices	Travelling personnel requested to decrypt mobile devices for inspection or from whom mobile devices are taken out of sight by border control MUST report the potential compromise of classified information or the device to an ITSM as soon as possible.	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
22.3.5.C.01	Storage requirements	Agencies MUST ensure that when mobile devices are not being actively used they are secured in accordance with the minimum physical security requirements as stated in the PSR.	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
22.3.6.C.01	Processing requirements	Agencies MUST ensure that the area within which mobile devices are used meets the minimum physical security requirements as stated in the PSR.	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
22.4.7.C.01	Risk Assessment	Agencies MUST undertake a risk assessment and implement appropriate controls BEFORE implementing a BYOD Policy and permitting the use of BYOD.	Functional	Intersects With	Risk Assessment	RSK-04	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	
22.4.7.C.02	Risk Assessment	Agencies MUST take an integrated approach to BYOD security, covering policy, training, support, systems architecture, security, systems management, change management, incident detection & management and business continuity.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.8.C.01	Applicability and Usage	BYOD MUST only be permitted for agency information systems up to and including RESTRICTED.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.8.C.02	Applicability and Usage	BYOD MUST NOT be used for CONFIDENTIAL, SECRET or TOP SECRET systems.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.9.C.01	Technical Controls	Devices that have been "jail-broken", "rooted" or have settings violations MUST NOT be used for any agency business or be allowed to connect to any agency systems UNLESS this been specifically authorised.	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
22.4.10.C.01	BYOD Policy	Agencies may identify additional policy provisions and controls that are required, based on their assessment of risk. Agencies MUST implement the additional controls and protocols before implementing BYOD.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.10.C.02	BYOD Policy	Agencies MUST implement a BYOD acceptable use policy, agreed and signed by each person using a BYOD device.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.10.C.03	BYOD Policy	The agency's policy MUST clearly establish eligibility of personnel for participation in the agency BYOD scheme.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.10.C.04	BYOD Policy	Personnel MUST have written authorisation (usually managerial approval) before a connection is enabled (on-boarding).	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.10.C.05	BYOD Policy	Written authorisation MUST include the nature and extent of agency access approved, considering: time, day of the week; location; and local or roaming access.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.10.C.06	BYOD Policy	Procedures MUST be established for removal of agency installed software and any agency data when the user no longer has a need to use BYOD, is redeployed or ceases employment (off-boarding).	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.10.C.07	BYOD Policy	Standard Operating Procedures for the agency's BYOD network MUST be established.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.10.C.08	BYOD Policy	Provision MUST be made for contractors and other authorised non-employees. It is at the agency's discretion whether this activity is permitted. The risk assessment MUST reflect this factor.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.10.C.09	BYOD Policy	Ownership of data on BYOD devices MUST be clearly articulated and agreed.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.10.C.10	BYOD Policy	Agency policies MUST clearly articulate the separation between corporate support and where individuals are responsible for the maintenance and support of their own devices.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.10.C.11	BYOD Policy	Agency policies MUST clearly articulate the acceptable use of any GPS or other tracking capability.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.10.C.12	BYOD Policy	Individual responsibility for the cost of any BYOD device and its accessories MUST be agreed.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.10.C.13	BYOD Policy	Individual responsibility for replacement in the event of loss or theft MUST be agreed.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.10.C.14	BYOD Policy	Individuals MUST be responsible for the installation and maintenance of any mandated BYOD-based firewalls and anti-malware software and for implementing operating system updates and patches on their device.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.10.C.15	BYOD Policy	The procedures for purchasing and installing business related applications on the mobile devices MUST be specified and agreed.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.10.C.16	BYOD Policy	The responsibility for payment of voice and data plans and roaming charges MUST be specified and agreed.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.11.C.01	BYOD Infrastructure and System Controls	A security architectural review MUST be undertaken by the agency before allowing BYOD devices to connect to agency systems.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.11.C.02	BYOD Infrastructure and System Controls	The BYOD network segment MUST be segregated from other elements of the agency's network.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.11.C.03	BYOD Infrastructure and System Controls	Agencies MUST architecturally separate guest and public facing networks from BYOD networks.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.11.C.04	BYOD Infrastructure and System Controls	Network configuration policies and authentication mechanisms MUST allow access to agency resources ONLY through the BYOD network segment.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.11.C.05	BYOD Infrastructure and System Controls	Access to internal resources and servers MUST be carefully managed and confined to only those services for which there is a defined and properly authorised business requirement.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.11.C.06	BYOD Infrastructure and System Controls	Wireless access points used for access to agency networks MUST be implemented and secured in accordance with the directions in this manual (See Section 18.2 - Wireless Local Area Networks).	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
22.4.11.C.07	BYOD Infrastructure and System Controls	Bluetooth on BYOD devices MUST be disabled while within designated secure areas on agency premises.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.11.C.08	BYOD Infrastructure and System Controls	Access Controls MUST be implemented in accordance with Chapter 16 - Access Control.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.11.C.09	BYOD Infrastructure and System Controls	Agencies MUST maintain a list of permitted operating systems, including operating system version numbers, for BYOD devices.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.11.C.10	BYOD Infrastructure and System Controls	Agencies MUST check each BYOD device for malware and sanitise the device appropriately before installing agency software or operating environments.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.11.C.11	BYOD Infrastructure and System Controls	Agencies MUST check each BYOD device for malware and sanitise the device appropriately before permitting access to agency data.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.11.C.12	BYOD Infrastructure and System Controls	BYOD MUST have a Mobile Device Management (MDM) solution implemented with a minimum of the following enabled: The MDM is enabled to "wipe" devices of any agency data if lost or stolen; If the MDM cannot discriminate between agency and personal data, all data, including personal data, is deleted if the device is lost or stolen; The MDM is capable of remotely applying agency security configurations for BYOD devices; Mobile device security configurations are validated (health check) by the MDM before a device is permitted to connect to the agency's systems; "Jail-broken", "rooted" or settings violations MUST be detected and isolated; "Jail-broken" devices are NOT permitted to access agency resources; Access to agency resources is limited until both the device and user is fully compliant with policy and SOPs; Auditing and logging is enabled; and Changes of Subscriber Identity Module (SIM) card are monitored to allow remote blocking and wiping in the event of theft or compromise.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.11.C.13	BYOD Infrastructure and System Controls	Intrusion detection systems MUST be implemented.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.11.C.14	BYOD Infrastructure and System Controls	Continuous monitoring MUST be established to detect actual or potential security compromises or incidents from BYOD devices. Refer also to Chapter 6 - Information Security Monitoring.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.11.C.15	BYOD Infrastructure and System Controls	Agencies MUST maintain a list of approved cloud applications that may be used on BYOD devices.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.11.C.16	BYOD Infrastructure and System Controls	Agencies MUST block the use of unapproved cloud applications for processing any agency or organisational data.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.11.C.17	BYOD Infrastructure and System Controls	BYOD devices MUST NOT be permitted direct connection to internal hosts, including all other devices on the local network.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.11.C.18	BYOD Infrastructure and System Controls	BYOD devices connecting to guest and public facing networks MUST NOT be permitted access to the corporate network other than through a VPN over the Internet.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.11.C.19	BYOD Infrastructure and System Controls	Bluetooth on BYOD devices SHOULD be disabled while within agency premises and while accessing agency systems and data.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.11.C.20	BYOD Infrastructure and System Controls	BYOD devices and systems SHOULD use Multi-factor (at least two-factor) authentication to connect to agency systems and prior to being permitted access to agency data.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.12.C.01	Wireless IDS / IPS systems	Agencies MUST implement a wireless IDS /IPS on BYOD wireless networks.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.12.C.02	Wireless IDS / IPS systems	Agencies MUST implement rogue AP and wireless "hot spot" detection and implement response procedures where detection occurs.	Functional	Intersects With	Rogue Wireless Detection	NET-15.5	Mechanisms exist to test for the presence of Wireless Access Points (WAPs) and identify all authorized and unauthorized WAPs within the facility(ies).	5	
22.4.12.C.03	Wireless IDS / IPS systems	Agencies SHOULD conduct a baseline survey to identify: All authorised devices and APs; and Any unauthorised devices and APs.	Functional	Intersects With	Rogue Wireless Detection	NET-15.5	Mechanisms exist to test for the presence of Wireless Access Points (WAPs) and identify all authorized and unauthorized WAPs within the facility(ies).	5	
22.4.13.C.01	BYOD Device Controls	Any agency data exchanged with the mobile device MUST be encrypted in transit (See Chapter 17 - Cryptography).	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.13.C.02	BYOD Device Controls	Any agency data stored on the device MUST be encrypted (including keys, certificates and other essential session establishment data).	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.13.C.03	BYOD Device Controls	The use of virtual containers, sandboxes, wraps or similar mechanisms on the mobile device MUST be established for each authorised session for any organisational data. These mechanisms MUST be non-persistent and be removed at the end of each session.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.13.C.04	BYOD Device Controls	Any sensitive agency data MUST be removed and securely deleted, or encrypted at the end of a session.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.13.C.05	BYOD Device Controls	Connections to the agency network MUST be time limited to avoid leaving a session "logged on".	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.13.C.06	BYOD Device Controls	Communications between the mobile device and the agency network MUST be established through a Virtual Private Network (VPN).	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.13.C.07	BYOD Device Controls	Agencies MUST disable split-tunnelling when using a BYOD device to connect to an agency network (See Section 21.1 - Agency Owned Mobile Devices).	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.13.C.08	BYOD Device Controls	Agencies MUST disable the ability for a BYOD device to establish simultaneous connections (e.g. wireless and cellular) when connected to an agency's network.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.13.C.09	BYOD Device Controls	The use of passwords or PINs to unlock the BYOD device MUST be enforced in addition to all other agency authentication mechanisms.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.13.C.10	BYOD Device Controls	BYOD device passwords MUST be distinct from any agency access and authentication passwords.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.13.C.11	BYOD Device Controls	BYOD passwords MUST be distinct from other fixed or mobile agency network passwords (See Section 16.1 - Identification and Authentication for details on password requirements).	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.14.C.01	Additional Controls	Agencies SHOULD compile a list of approved BYOD devices and operating systems for the guidance of staff.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.14.C.02	Additional Controls	Agencies SHOULD consider the implementation of Data Loss Prevention (DLP) technologies.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.14.C.03	Additional Controls	Agencies SHOULD consider the use of bandwidth limits as a means of controlling data downloads and uploads.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
22.4.14.C.04	Additional Controls	Agencies SHOULD take legal advice on the provisions in their BYOD policy.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
23.1.54.C.01	Cloud security boundaries	Agencies MUST clearly identify and understand where classification, security domain, and trust zone boundaries exist prior to implementation or adoption of public cloud services.	Functional	Subset Of	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	10	
23.1.54.C.01	Cloud security boundaries	Agencies MUST clearly identify and understand where classification, security domain, and trust zone boundaries exist prior to implementation or adoption of public cloud services.	Functional	Intersects With	Cloud Security Architecture	CLD-02	Mechanisms exist to ensure the cloud security architecture supports the organization's technology strategy to securely design, configure and maintain cloud employments.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
23.1.54.C.02	Cloud security boundaries	Where multiple identity systems under different security policies are used to control access to an agency's instance of a public cloud service, the instance MUST be considered to be in a separate security domain from services where access control is managed solely by the agency's identity system.	Functional	Subset Of	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	10	
23.1.54.C.02	Cloud security boundaries	Where multiple identity systems under different security policies are used to control access to an agency's instance of a public cloud service, the instance MUST be considered to be in a separate security domain from services where access control is managed solely by the agency's identity system.	Functional	Intersects With	Cloud Security Architecture	CLD-02	Mechanisms exist to ensure the cloud security architecture supports the organization's technology strategy to securely design, configure and maintain cloud employments.	5	
23.1.55.C.01	Shared responsibility model	Agencies MUST clearly identify and understand their cloud service providers security responsibilities for each service consumed, and the aspects of security that the agency is responsible for, prior to implementation or adoption of the service.	Functional	Intersects With	Multi-Tenant Environments	CLD-06	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	5	
23.1.55.C.01	Shared responsibility model	Agencies MUST clearly identify and understand their cloud service providers security responsibilities for each service consumed, and the aspects of security that the agency is responsible for, prior to implementation or adoption of the service.	Functional	Intersects With	Customer Responsibility Matrix (CRM)	CLD-06.1	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.	5	
23.1.55.C.02	Shared responsibility model	Agencies SHOULD clearly document the aspects of security they and their provider are responsible for.	Functional	Intersects With	Multi-Tenant Environments	CLD-06	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	5	
23.1.55.C.02	Shared responsibility model	Agencies SHOULD clearly document the aspects of security they and their provider are responsible for.	Functional	Intersects With	Customer Responsibility Matrix (CRM)	CLD-06.1	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.	5	
23.1.55.C.03	Shared responsibility model	Agencies SHOULD review existing security processes to ensure compatibility with their cloud service providers responsibilities.	Functional	Intersects With	Multi-Tenant Environments	CLD-06	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	5	
23.1.55.C.03	Shared responsibility model	Agencies SHOULD review existing security processes to ensure compatibility with their cloud service providers responsibilities.	Functional	Intersects With	Customer Responsibility Matrix (CRM)	CLD-06.1	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.	5	
23.1.56.C.01	Automation and infrastructure as code	Agencies SHOULD deploy and manage their cloud infrastructure using automation, version control, and infrastructure as code techniques where these are available.	Functional	Intersects With	Cloud Security Architecture	CLD-02	Mechanisms exist to ensure the cloud security architecture supports the organization's technology strategy to securely design, configure and maintain cloud employments.	5	
23.2.16.C.01	Understanding levels of assurance for public cloud	Agencies MUST update their risk assessment process to account for public cloud specific risks, prior to implementation or adoption of public cloud services.	Functional	Intersects With	Risk Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
23.2.16.C.01	Understanding levels of assurance for public cloud	Agencies MUST update their risk assessment process to account for public cloud specific risks, prior to implementation or adoption of public cloud services.	Functional	Intersects With	Impact-Level Prioritization	RSK-02.1	Mechanisms exist to prioritize the impact level for Technology Assets, Applications and/or Services (TAAS) to prevent potential disruptions.	5	
23.2.16.C.02	Understanding levels of assurance for public cloud	Agencies MUST undertake a cloud specific risk assessment in line with the process outlined by the GCDO for each public cloud service, prior to implementation or adoption of public cloud services.	Functional	Intersects With	Risk Assessment	RSK-04	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	
23.2.16.C.03	Understanding levels of assurance for public cloud	Agencies MUST NOT accredit public cloud services for use with data classified CONFIDENTIAL, SECRET, or TOP SECRET.	Functional	Intersects With	Authorize Technology Assets, Applications and/or Services (TAAS)	GOV-15.4	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	
23.2.16.C.03	Understanding levels of assurance for public cloud	Agencies MUST NOT accredit public cloud services for use with data classified CONFIDENTIAL, SECRET, or TOP SECRET.	Functional	Intersects With	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	5	
23.2.16.C.04	Understanding levels of assurance for public cloud	Agencies MUST NOT accredit public cloud services to host, process, store, or transmit NZEO endorsed information.	Functional	Intersects With	Authorize Technology Assets, Applications and/or Services (TAAS)	GOV-15.4	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	
23.2.16.C.04	Understanding levels of assurance for public cloud	Agencies MUST NOT accredit public cloud services to host, process, store, or transmit NZEO endorsed information.	Functional	Intersects With	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	5	
23.2.17.C.01	System availability	Agencies MUST consider risks to the availability of systems and information in their design of cloud systems architectures, supporting controls, and governance processes prior to implementation or adoption of public cloud services.	Functional	Intersects With	Risk Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
23.2.17.C.01	System availability	Agencies MUST consider risks to the availability of systems and information in their design of cloud systems architectures, supporting controls, and governance processes prior to implementation or adoption of public cloud services.	Functional	Intersects With	Impact-Level Prioritization	RSK-02.1	Mechanisms exist to prioritize the impact level for Technology Assets, Applications and/or Services (TAAS) to prevent potential disruptions.	5	
23.2.18.C.01	Regular assurance checks	Agencies SHOULD obtain regular assurance checks on cloud service providers, ensuring they have been undertaken by a suitably qualified assessor.	Functional	Intersects With	Monitor Controls	GOV-15.5	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	
23.2.18.C.01	Regular assurance checks	Agencies SHOULD obtain regular assurance checks on cloud service providers, ensuring they have been undertaken by a suitably qualified assessor.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
23.2.18.C.01	Regular assurance checks	Agencies SHOULD obtain regular assurance checks on cloud service providers, ensuring they have been undertaken by a suitably qualified assessor.	Functional	Intersects With	Control Conformity Monitoring	CPL-03	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	
23.2.18.C.01	Regular assurance checks	Agencies SHOULD obtain regular assurance checks on cloud service providers, ensuring they have been undertaken by a suitably qualified assessor.	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	5	
23.2.19.C.01	Cloud service providers - patching and software maintenance	Agencies MUST obtain assurance that cloud service providers undertake appropriate software and operating system patching and maintenance.	Functional	Subset Of	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	10	
23.2.19.C.01	Cloud service providers - patching and software maintenance	Agencies MUST obtain assurance that cloud service providers undertake appropriate software and operating system patching and maintenance.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
23.2.19.C.01	Cloud service providers - patching and software maintenance	Agencies MUST obtain assurance that cloud service providers undertake appropriate software and operating system patching and maintenance.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	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	
23.2.19.C.01	Cloud service providers - patching and software maintenance	Agencies MUST obtain assurance that cloud service providers undertake appropriate software and operating system patching and maintenance.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
23.2.19.C.01	Cloud service providers - patching and software maintenance	Agencies MUST obtain assurance that cloud service providers undertake appropriate software and operating system patching and maintenance.	Functional	Intersects With	Continuous Vulnerability Remediation Activities	VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	5	
23.2.19.C.01	Cloud service providers - patching and software maintenance	Agencies MUST obtain assurance that cloud service providers undertake appropriate software and operating system patching and maintenance.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	
23.2.20.C.01	Assurance around workload isolation on shared infrastructure	Agencies MUST obtain assurance that technical protections exist to adequately isolate tenants.	Functional	Intersects With	Cloud Security Architecture	CLD-02	Mechanisms exist to ensure the cloud security architecture supports the organization's technology strategy to securely design, configure and maintain cloud employments.	5	
23.2.20.C.01	Assurance around workload isolation on shared infrastructure	Agencies MUST obtain assurance that technical protections exist to adequately isolate tenants.	Functional	Intersects With	Multi-Tenant Environments	CLD-06	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
23.2.21.C.01	Use of baseline security templates	Agencies SHOULD make use of the GCSB endorsed baseline security templates where applicable.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
23.2.21.C.01	Use of baseline security templates	Agencies SHOULD make use of the GCSB endorsed baseline security templates where applicable.	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	5	
23.3.18.C.01	Privileged account separation	Accounts used to perform privileged actions SHOULD NOT be synchronised between environments.	Functional	Intersects With	Privileged Account Separation	IAC-16.2	Mechanisms exist to separate privileged accounts between infrastructure environments to reduce the risk of a compromise in one infrastructure environment from laterally affecting other infrastructure environments.	5	
23.3.19.C.01	Username and passwords	Where administration interfaces or portals are accessible from the internet, privileged accounts MUST be configured to use multiple factors of authentication.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5	
23.3.19.C.02	Username and passwords	Where cloud service interfaces or portals are accessible from the internet, user accounts SHOULD be configured to use multiple factors of authentication.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5	
23.3.20.C.01	Offboarding	Staff offboarding processes MUST be updated to include removing all access to public cloud based services, prior to implementation or adoption of public cloud services.	Functional	Intersects With	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	5	
23.3.21.C.01	Authentication	Agencies MUST ensure that relying parties continually verify the authenticity of their identity providers responses, through for example, cryptographic signing of authentication requests and responses.	Functional	Intersects With	Public Key Infrastructure (PKI)	CRY-08	Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service provider.	5	
23.3.21.C.01	Authentication	Agencies MUST ensure that relying parties continually verify the authenticity of their identity providers responses, through for example, cryptographic signing of authentication requests and responses.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
23.3.21.C.01	Authentication	Agencies MUST ensure that relying parties continually verify the authenticity of their identity providers responses, through for example, cryptographic signing of authentication requests and responses.	Functional	Intersects With	Certificate Authorities	CRY-11	Automated mechanisms exist to enable the use of organization-defined Certificate Authorities (CAs) to facilitate the establishment of protected sessions.	5	
23.3.22.C.01	Relying parties	Agencies SHOULD ensure that relying parties use all available information from the identity provider to inform access control decisions.	Functional	Intersects With	Public Key Infrastructure (PKI)	CRY-08	Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service provider.	5	
23.3.22.C.01	Relying parties	Agencies SHOULD ensure that relying parties use all available information from the identity provider to inform access control decisions.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
23.3.22.C.01	Relying parties	Agencies SHOULD ensure that relying parties use all available information from the identity provider to inform access control decisions.	Functional	Intersects With	Certificate Authorities	CRY-11	Automated mechanisms exist to enable the use of organization-defined Certificate Authorities (CAs) to facilitate the establishment of protected sessions.	5	
23.4.9.C.01	Data protection mechanisms	For each cloud service, agencies MUST ensure that the mechanisms used to protect data meet agency requirements.	Functional	Intersects With	Cloud Infrastructure Onboarding	CLD-01.1	Mechanisms exist to ensure cloud services are designed and configured so Technology Assets, Applications and/or Services (TAAS) are secured in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	
23.4.9.C.02	Data protection mechanisms	Agencies MUST update key management plans to account for differences in public cloud before storing organisational data in a public cloud environment.	Functional	Intersects With	Cloud Infrastructure Onboarding	CLD-01.1	Mechanisms exist to ensure cloud services are designed and configured so Technology Assets, Applications and/or Services (TAAS) are secured in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	
23.4.9.C.02	Data protection mechanisms	Agencies MUST update key management plans to account for differences in public cloud before storing organisational data in a public cloud environment.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
23.4.9.C.02	Data protection mechanisms	Agencies MUST update key management plans to account for differences in public cloud before storing organisational data in a public cloud environment.	Functional	Intersects With	External System Cryptographic Key Control	CRY-09.7	Mechanisms exist to maintain control of cryptographic keys for encrypted material stored or transmitted through an external system.	5	
23.4.9.C.03	Data protection mechanisms	Agencies MUST ensure their key management plan includes provision for migrating data from the cloud environment where it was created.	Functional	Intersects With	Cloud Infrastructure Onboarding	CLD-01.1	Mechanisms exist to ensure cloud services are designed and configured so Technology Assets, Applications and/or Services (TAAS) are secured in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	
23.4.9.C.03	Data protection mechanisms	Agencies MUST ensure their key management plan includes provision for migrating data from the cloud environment where it was created.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
23.4.9.C.03	Data protection mechanisms	Agencies MUST ensure their key management plan includes provision for migrating data from the cloud environment where it was created.	Functional	Intersects With	External System Cryptographic Key Control	CRY-09.7	Mechanisms exist to maintain control of cryptographic keys for encrypted material stored or transmitted through an external system.	5	
23.4.10.C.01	Data accessibility	Agencies MUST apply the principle of least privilege and configure service endpoints to restrict access to authorised parties.	Functional	Intersects With	Cloud Infrastructure Onboarding	CLD-01.1	Mechanisms exist to ensure cloud services are designed and configured so Technology Assets, Applications and/or Services (TAAS) are secured in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	
23.4.10.C.01	Data accessibility	Agencies MUST apply the principle of least privilege and configure service endpoints to restrict access to authorised parties.	Functional	Intersects With	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
23.4.11.C.01	Data location	Agencies MUST identify where data used in conjunction with a public cloud service is stored or processed, including any replicas or backups that may be created.	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	CLD-09	Mechanisms exist to control the location of cloud processing/storage based on business requirements that includes statutory, regulatory and contractual obligations.	5	
23.4.11.C.02	Data location	Agency risk assessments of public cloud services MUST include any risks arising from data location. Any actions required to mitigate these risks must be identified and documented prior to implementation or adoption of public cloud services.	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	CLD-09	Mechanisms exist to control the location of cloud processing/storage based on business requirements that includes statutory, regulatory and contractual obligations.	5	
23.4.12.C.01	Revise disaster recovery plans to include data in public cloud	Agencies MUST update their disaster recovery plans prior to storing or replicating data in public cloud services, to ensure these plans address any cloud-specific aspects of backup and recovery.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
23.4.12.C.02	Revise disaster recovery plans to include data in public cloud	When planning tests of disaster recovery processes in accordance with 6.4.6 Backup strategy, agencies MUST include tests of any cloud-specific data recovery processes.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
23.4.13.C.01	Data retrieval and removal	Agencies MUST have a defined exit strategy for each public cloud service they consume, including a process by which their data can be retrieved and erased from the cloud service as part of contract termination.	Functional	Intersects With	Cloud Infrastructure Offboarding	CLD-01.2	Mechanisms exist to ensure cloud services are decommissioned so that data is securely transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	
23.4.13.C.02	Data retrieval and removal	Agencies MUST ensure all data they need to retain is retrieved from the cloud service provider prior to decommissioning.	Functional	Intersects With	Cloud Infrastructure Offboarding	CLD-01.2	Mechanisms exist to ensure cloud services are decommissioned so that data is securely transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	
23.4.13.C.03	Data retrieval and removal	Agencies MUST have assurance that no agency-owned data is retained on the cloud service being decommissioned.	Functional	Intersects With	Cloud Infrastructure Offboarding	CLD-01.2	Mechanisms exist to ensure cloud services are decommissioned so that data is securely transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	
23.5.10.C.01	Logging public cloud events	Agencies MUST understand the range of logging capabilities provided by their cloud service providers and determine whether they are sufficient for agency needs.	Functional	Intersects With	Assessment Boundaries	IAO-01.1	Mechanisms exist to establish the scope of assessments by defining the assessment boundary, according to people, processes and technology that directly or indirectly impact the confidentiality, integrity, availability and safety of the Technology Assets, Applications, Services and/or Data (TAASD) under review.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: New Zealand - Information Security Manual (ISM) v3.9
Focal Document URL: https://www.nzism.gcsb.govt.nz/ism-document/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-ism-3-9.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
23.5.10.C.01	Logging public cloud events	Agencies MUST understand the range of logging capabilities provided by their cloud service providers and determine whether they are sufficient for agency needs.	Functional	Intersects With	Assessments	IAO-02	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	
23.5.11.C.01	Logging requirements	Agencies MUST ensure that logs associated with public cloud services are collected, protected, and that their integrity can be confirmed in accordance with the agency's documented logging requirements.	Functional	Intersects With	Cloud Infrastructure Onboarding	CLD-01.1	Mechanisms exist to ensure cloud services are designed and configured so Technology Assets, Applications and/or Services (TAAS) are secured in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	
23.5.11.C.01	Logging requirements	Agencies MUST ensure that logs associated with public cloud services are collected, protected, and that their integrity can be confirmed in accordance with the agency's documented logging requirements.	Functional	Intersects With	Multi-Tenant Event Logging Capabilities	CLD-06.2	Mechanisms exist to ensure Multi-Tenant Service Providers (MTSP) facilitate security event logging capabilities for its customers that are consistent with applicable statutory, regulatory and/or contractual obligations.	5	
23.5.12.C.01	Detecting information security incidents in public cloud	Agencies MUST ensure that cloud service provider logs are incorporated into overall enterprise logging and alerting systems or procedures in a timely manner to detect information security incidents.	Functional	Intersects With	Cloud Infrastructure Onboarding	CLD-01.1	Mechanisms exist to ensure cloud services are designed and configured so Technology Assets, Applications and/or Services (TAAS) are secured in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	
23.5.12.C.01	Detecting information security incidents in public cloud	Agencies MUST ensure that cloud service provider logs are incorporated into overall enterprise logging and alerting systems or procedures in a timely manner to detect information security incidents.	Functional	Intersects With	Multi-Tenant Event Logging Capabilities	CLD-06.2	Mechanisms exist to ensure Multi-Tenant Service Providers (MTSP) facilitate security event logging capabilities for its customers that are consistent with applicable statutory, regulatory and/or contractual obligations.	5	
23.5.12.C.01	Detecting information security incidents in public cloud	Agencies MUST ensure that cloud service provider logs are incorporated into overall enterprise logging and alerting systems or procedures in a timely manner to detect information security incidents.	Functional	Intersects With	Multi-Tenant Incident Response Capabilities	CLD-06.4	Mechanisms exist to ensure Multi-Tenant Service Providers (MTSP) facilitate prompt response to suspected or confirmed security incidents and vulnerabilities, including timely notification to affected customers.	5	
23.5.12.C.02	Detecting information security incidents in public cloud	Agencies SHOULD ensure that tools and procedures used to detect potential information security incidents account for the public cloud services being consumed by the agency.	Functional	Intersects With	Cloud Infrastructure Onboarding	CLD-01.1	Mechanisms exist to ensure cloud services are designed and configured so Technology Assets, Applications and/or Services (TAAS) are secured in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	