NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference document: Secure Controls Framework (SCF) version 2026.1
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document: **HISO 10029:2025 NZ Health Information Security Framework (HISF) - MicroSmall (2023)**
Focal Document URL: https://www.tewhatuora.govt.nz/publications/health-information-security-framework/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-nzl-hisf-microsmall-2023.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
HMS01	Governance - Information security roles and responsibilities	Information security roles and responsibilities are to be clearly defined.	Functional	Equal	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
HMS02	Governance - Policies for information security	A defined health information security policy is documented and approved by management.	Functional	Equal	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	
HMS03	Asset Management - Inventory of information and assets	An inventory of assets where health information is stored, including software, endpoint devices and relevant owners are identified and maintained.	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	
HMS03	Asset Management - Inventory of information and assets	An inventory of assets where health information is stored, including software, endpoint devices and relevant owners are identified and maintained.	Functional	Intersects With	Sensitive Data Inventories	DCH-06.2	Mechanisms exist to maintain inventory logs of all sensitive media and conduct sensitive media inventories at least annually.	5	
HMS04	Supplier Management - Supply Chain Risk Management	All suppliers responsible for delivering health information related assets and services are to undergo periodic security assurance activities.	Functional	Equal	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	10	
HMS05	Risk Management - Information Security Risk Assessment	A security risk assessment is conducted periodically, and the identified risks are managed.	Functional	Equal	Risk Assessment Update	RSK-07	Mechanisms exist to routinely update risk assessments and react accordingly upon identifying new security vulnerabilities, including using outside sources for security vulnerability information.	10	
HMS06	Information Sharing - Protection of health information	Requirements are identified, and contractual obligations are met before the information is shared with authorised parties.	Functional	Equal	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).	10	
HMS07	Access Management - Access Control and Secure Authentication	Access to health information and endpoint devices is provided based on the legitimate business and health information security requirements and on the role of the individual.	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	
HMS07	Access Management - Access Control and Secure Authentication	Access to health information and endpoint devices is provided based on the legitimate business and health information security requirements and on the role of the individual.	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5	
HMS08	Device Management - Management of Technical Vulnerabilities	Latest operating systems, hardware devices, relevant software and internet browsers are used and kept up-to-date and where applicable, licensed versions are to be used.	Functional	Equal	Stable Versions	VPM-04.1	Mechanisms exist to install the latest stable version of any software and/or security-related updates on all applicable systems.	10	
HMS09	Device Management - Installation of software on operational systems	Permissions for all personnel is restricted so that external media, unauthorised or malicious software is not installed on devices that are used to store, process or transfer health information.	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	
HMS09	Device Management - Installation of software on operational systems	Permissions for all personnel is restricted so that external media, unauthorised or malicious software is not installed on devices that are used to store, process or transfer health information.	Functional	Intersects With	Removable Media Security	DCH-12	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	5	
HMS09	Device Management - Installation of software on operational systems	Permissions for all personnel is restricted so that external media, unauthorised or malicious software is not installed on devices that are used to store, process or transfer health information.	Functional	Intersects With	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	5	
HMS10	Device Management - Protection against malware	Up-to-date anti-virus, anti-malware/endpoint security software is installed on all computers and servers to protect health information and endpoint devices against malicious code or software.	Functional	Equal	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	10	
HMS11	Device Management - Information backup	All relevant health information is backed up securely (as outlined in your documented policy) in an encrypted format and restoration is tested periodically.	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	
HMS11	Device Management - Information backup	All relevant health information is backed up securely (as outlined in your documented policy) in an encrypted format and restoration is tested periodically.	Functional	Intersects With	Testing for Reliability & Integrity	BCD-11.1	Mechanisms exist to routinely test backups that verify the reliability of the backup process, as well as the integrity and availability of the data.	5	
HMS11	Device Management - Information backup	All relevant health information is backed up securely (as outlined in your documented policy) in an encrypted format and restoration is tested periodically.	Functional	Intersects With	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	5	
HMS12	Device Management - User endpoint devices	Only authorised devices that are managed and have security controls in place are to be used to process health information.	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	
HMS12	Device Management - User endpoint devices	Only authorised devices that are managed and have security controls in place are to be used to process health information.	Functional	Intersects With	Approved Technologies	AST-01.4	Mechanisms exist to maintain a current list of approved technologies (hardware and software).	5	
HMS13	Device Management - Remote working	When personnel are working remotely, security measures are in place to protect health information which could be accessed, processed, or stored outside the organisations premises.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	
HMS13	Device Management - Remote working	When personnel are working remotely, security measures are in place to protect health information which could be accessed, processed, or stored outside the organisations premises.	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	
HMS14	Information Sharing - Data Leakage Prevention	Licensed and secure software, tools or services are used to manage health information.	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	
HMS14	Information Sharing - Data Leakage Prevention	Licensed and secure software, tools or services are used to manage health information.	Functional	Intersects With	Software Licensing Restrictions	AST-02.7	Mechanisms exist to protect Intellectual Property (IP) rights with software licensing restrictions.	5	
HMS15	Network Management - Security of networks	Network services used for transmitting and receiving health information and data are kept secure, to ensure minimal security impact upon clinical practice.	Functional	Equal	Sensitive / Regulated Data Enclave (Secure Zone)	NET-06.3	Mechanisms exist to implement segmentation controls to restrict inbound and outbound connectivity for sensitive/regulated data enclaves (secure zones).	10	
HMS16	Network Management - Separation of networks	Devices processing or storing or transmitting health information are connected, where possible, to a separate network with heightened security away from other information and assets.	Functional	Equal	Isolation of System Components	NET-03.7	Mechanisms exist to employ boundary protections to isolate Technology Assets, Applications and/or Services (TAAS) that support critical missions and/or business functions.	10	
HMS17	Operations Security - Encryption	Web traffic is encrypted for public facing websites which contain health information, so that they are protected against Distributed Denial of Service (DDoS) attacks.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5	
HMS17	Operations Security - Encryption	Web traffic is encrypted for public facing websites which contain health information, so that they are protected against Distributed Denial of Service (DDoS) attacks.	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	
HMS18	Operations Security - Logging	All health information user activities are recorded, stored for a period of time and protected for analysis in case of a security incident.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
HMS18	Operations Security - Logging	All health information user activities are recorded, stored for a period of time and protected for analysis in case of a security incident.	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	
HMS19	Operations Security - Real time monitoring	Unusual behaviour and potential information security incidents amongst endpoints and internal and external network traffic are detected.	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	
HMS19	Operations Security - Real time monitoring	Unusual behaviour and potential information security incidents amongst endpoints and internal and external network traffic are detected.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5	
HMS20	Incident Management - Information security incident management planning and preparation	A documented and approved security incident management process is maintained, reviewed, and tested periodically.	Functional	Equal	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	10	
HMS21	Business Continuity Management - ICT readiness for business continuity	Availability of health information is to be maintained in the event of a service, system, or application being disrupted for a prolonged period.	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	