NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document : Secure Controls Framework (SCF) version 2025.1
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document: **HISO 10029:2024 NZ Health Information Security Framework Guidance for Suppliers**
Focal Document URL: https://www.tewhatuora.govt.nz/assets/Publications/HISO-Standards/HISO-10029-4-2023-Health-Information-Security-Framework-Guidance-for-Suppliers.pdf
Published STRM URL: https://securecontrolsframework.com/content/strm/scf-strm-apac-nz-hisf-suppliers-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 (optional)	Notes (optional)
HSUP01	Information Security Policy - Policies for information security	The organisation has a clear information security policy, acceptable use policy, topic-specific policies and procedures to maintain information security.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
HSUP01	Information Security Policy - Policies for information security	The organisation has a clear information security policy, acceptable use policy, topic-specific policies and procedures to maintain information 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	
HSUP01	Information Security Policy - Policies for information security	The organisation has a clear information security policy, acceptable use policy, topic-specific policies and procedures to maintain information security.	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	
HSUP02	Human Resource Security - Terms and conditions of employment	Security roles and responsibilities of personnel are included within job descriptions.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
HSUP02	Human Resource Security - Terms and conditions of employment	Security roles and responsibilities of personnel are included within job descriptions.	Functional	Intersects With	Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
HSUP03	Human Resource Security - Terms and conditions of employment	A breach of information by personnel is considered a security policy violation. Consequences of a security policy violation leads to a disciplinary process.	Functional	Intersects With	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	5	
HSUP03	Human Resource Security - Terms and conditions of employment	A breach of information by personnel is considered a security policy violation. Consequences of a security policy violation leads to a disciplinary process.	Functional	Intersects With	Workplace Investigations	HRS-07.1	Mechanisms exist to conduct employee misconduct investigations when there is reasonable assurance that a policy has been violated.	5	
HSUP04	Human Resource Security - Onboarding, offboarding and role change	There are documented procedures for providing and revoking logical, and physical access when personnel join, have a role change or leave the organisation.	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	
HSUP04	Human Resource Security - Onboarding, offboarding and role change	There are documented procedures for providing and revoking logical, and physical access when personnel join, have a role change or leave the organisation.	Functional	Intersects With	Change of Roles & Duties	IAC-07.1	Mechanisms exist to revoke user access rights following changes in personnel roles and duties, if no longer necessary or permitted.	5	
HSUP04	Human Resource Security - Onboarding, offboarding and role change	There are documented procedures for providing and revoking logical, and physical access when personnel join, have a role change or leave the organisation.	Functional	Intersects With	Termination of Employment	IAC-07.2	Mechanisms exist to revoke user access rights in a timely manner, upon termination of employment or contract.	5	
HSUP04	Human Resource Security - Onboarding, offboarding and role change	There are documented procedures for providing and revoking logical, and physical access when personnel join, have a role change or leave the organisation.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	5	
HSUP04	Human Resource Security - Onboarding, offboarding and role change	There are documented procedures for providing and revoking logical, and physical access when personnel join, have a role change or leave the organisation.	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	
HSUP04	Human Resource Security - Onboarding, offboarding and role change	There are documented procedures for providing and revoking logical, and physical access when personnel join, have a role change or leave the organisation.	Functional	Intersects With	Role-Based Physical Access	PES-02.1	Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual.	5	
HSUP05	Asset Lifecycle Security - Information and associated assets	Asset management process(es) are in place.	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	
HSUP06	Asset Lifecycle Security - Media Equipment Management, Decommissioning and Disposal	Processes are in place for media equipment management, decommissioning and secure disposal.	Functional	Equal	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	10	
HSUP07	Information Security Incident Management - Planning and preparation	An information security incident management process is in place.	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	
HSUP07	Information Security Incident Management - Planning and preparation	An information security incident management process is in place.	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	
HSUP08	Business Continuity and Disaster Recovery Management - Information security during disruption	Organisations have a documented, approved, business continuity and disaster recovery management, operational resilience policies and procedures in place.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
HSUP09	Identity and Access Management - Access control	Establish, document, approve, and implement rules to control physical and logical access to information and its assets.	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	
HSUP09	Identity and Access Management - Access control	Establish, document, approve, and implement rules to control physical and logical access to information and its assets.	Functional	Intersects With	Access To Information Systems	PES-03.4	Physical access control mechanisms exist to enforce physical access to critical information systems or sensitive/regulated data, in addition to the physical access controls for the facility.	5	
HSUP10	Information Security Governance - Ownership of Information Security	The organisation's Board or information security steering committee is accountable for information security governance.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
HSUP10	Information Security Governance - Ownership of Information Security	The organisation's Board or information security steering committee is accountable for information security governance.	Functional	Intersects With	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.	5	
HSUP11	Physical and Environmental Security - Policies and Procedures	A documented policy and supporting procedures for maintaining physical security within the organisation is in place.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
HSUP11	Physical and Environmental Security - Policies and Procedures	A documented policy and supporting procedures for maintaining physical security within the organisation is in place.	Functional	Intersects With	Site Security Plan (SitePlan)	PES-01.1	Mechanisms exist to document a Site Security Plan (SitePlan) for each server and communications room to summarize the implemented security controls to protect physical access to technology assets, as well as applicable risks and threats.	5	
HSUP12	Physical and Environmental Security - Clear Desk and Clear Screen Procedure	A documented and approved procedure to remove papers and removable storage from easily accessible areas is to be implemented.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
HSUP12	Physical and Environmental Security - Clear Desk and Clear Screen Procedure	A documented and approved procedure to remove papers and removable storage from easily accessible areas is to be implemented.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is stored.	5	
HSUP12	Physical and Environmental Security - Clear Desk and Clear Screen Procedure	A documented and approved procedure to remove papers and removable storage from easily accessible areas is to be implemented.	Functional	Intersects With	Removable Media Security	DCH-12	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	5	
HSUP13	Cloud Security - Cloud security policy & cloud security agreement (CSA)	Organisations have planned maintenance of information and services that are being provided to their customers via cloud services as per documented policies and agreements.	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	
HSUP14	Systems Acquisition, Development and Maintenance - Security while developing applications, products or services	Information systems are securely designed, and appropriate controls are implemented.	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
HSUP14	Systems Acquisition, Development and Maintenance - Security while developing applications, products or services	Information systems are securely designed, and appropriate controls are implemented.	Functional	Intersects With	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
HSUP14	Systems Acquisition, Development and Maintenance - Security while developing applications, products or services	Information systems are securely designed, and appropriate controls are implemented.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	10	
HSUP15	Information Backups - Policy and procedures	A backup and recovery procedure is in place.	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
HSUP15	Information Backups - Policy and procedures	A backup and recovery procedure is in place.	Functional	Intersects With	Information System Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of systems to a known state after a disruption, compromise or failure.	5	
HSUP15	Information Backups - Policy and procedures	A backup and recovery procedure is in place.	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
HSUP15	Information Backups - Policy and procedures	A backup and recovery procedure is in place.	Functional	Intersects With	Information System Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of systems to a known state after a disruption, compromise or failure.	5	
HSUP16	Change Management - Policy and procedures	A documented process is in place for performing changes to new and existing systems or services.	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
HSUP16	Change Management - Policy and procedures	A documented process is in place for performing changes to new and existing systems or services.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
HSUP17	Patch and Vulnerability Management - Policy and procedures	There is a documented and approved process for identifying vulnerabilities and updating patches on the organisation's systems, applications, tools, services etc.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
HSUP17	Patch and Vulnerability Management - Policy and procedures	There is a documented and approved process for identifying vulnerabilities and updating patches on the organisation's systems, applications, tools, services etc.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
HSUP17	Patch and Vulnerability Management - Policy and procedures	There is a documented and approved process for identifying vulnerabilities and updating patches on the organisation's systems, applications, tools, services etc.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	5	
HSUP18	Human Resource Security - Terms and conditions of employment	Organisations, at a minimum, screen all personnel by verifying their identity, previous employment, applicable professional qualifications and criminal backgrounds before confirmation of employment.	Functional	Equal	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	10	
HSUP19	Human Resource Security - Roles and responsibilities	Organisations are to ensure: a) information security responsibilities are clearly defined and assigned b) a governance body or steering committee overseeing information security activities is in place c) there is at least one individual responsible for maintaining information security within the organisation.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
HSUP19	Human Resource Security - Roles and responsibilities	Organisations are to ensure: a) information security responsibilities are clearly defined and assigned b) a governance body or steering committee overseeing information security activities is in place c) there is at least one individual responsible for maintaining information security within the organisation.	Functional	Intersects With	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
HSUP19	Human Resource Security - Roles and responsibilities	Organisations are to ensure: a) information security responsibilities are clearly defined and assigned b) a governance body or steering committee overseeing information security activities is in place c) there is at least one individual responsible for maintaining information security within the organisation.	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing data and technology-related risks.	5	
HSUP20	Human Resource Security - Training Requirements	There has been an assessment of information security training needs and a training plan is put in place.	Functional	Subset Of	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
HSUP21	Information Security Incident Management - Roles and Responsibilities	Organisations are to have roles and responsibilities determined to carry out the incident management process.	Functional	Equal	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
HSUP22	Business Continuity and Disaster Recovery Management - ICT readiness for business continuity	Establish criteria for developing business continuity, disaster recovery, operational resilience strategies, and capabilities based on disruption and impact to the organisation.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
HSUP22	Business Continuity and Disaster Recovery Management - ICT readiness for business continuity	Establish criteria for developing business continuity, disaster recovery, operational resilience strategies, and capabilities based on disruption and impact to the organisation.	Functional	Intersects With	Recovery Time / Point Objectives (RTO / RPO)	BCD-01.4	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
HSUP23	Information Security Governance - Roles and responsibilities	Roles and responsibilities are defined and documented for planning, implementing, operating, assessing, and reporting on the organisation's information security requirements.	Functional	Intersects With	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
HSUP23	Information Security Governance - Roles and responsibilities	Roles and responsibilities are defined and documented for planning, implementing, operating, assessing, and reporting on the organisation's information security requirements.	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing data and technology-related risks.	5	
HSUP24	Information Security Governance - Information security in project management	Organisations are to integrate information security into project management.	Functional	Intersects With	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
HSUP24	Information Security Governance - Information security in project management	Organisations are to integrate information security into project management.	Functional	Intersects With	Cybersecurity & Data Privacy In Project Management	PRM-04	Mechanisms exist to assess cybersecurity & data privacy controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.	5	
HSUP25	Compliance - Compliance requirements	Relevant legal, regulatory, and contractual requirements are identified and implemented.	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	
HSUP26	Cloud Security - Cloud security risk assessment and assurance	A risk assessment methodology and cloud assurance activities that support the use of cloud technologies are in place.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
HSUP27	Systems Acquisition, Development and Maintenance - Business, customer and security requirements	Business, customer, and security requirements are identified, documented, and approved when developing or acquiring applications.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical systems, applications and services to support the ongoing secure management of those assets.	5	
HSUP27	Systems Acquisition, Development and Maintenance - Business, customer and security requirements	Business, customer, and security requirements are identified, documented, and approved when developing or acquiring applications.	Functional	Intersects With	Cybersecurity & Data Privacy Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical systems, system components or services at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
HSUP27	Systems Acquisition, Development and Maintenance - Business, customer and security requirements	Business, customer, and security requirements are identified, documented, and approved when developing or acquiring applications.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity & data privacy 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	
HSUP28	Risk Management - Risk Assessments	Risk assessments are performed on new, existing systems, and applications to understand the risks posed to the organisation while using them.	Functional	Equal	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 systems and data.	10	
HSUP29	Change Management - Security testing	The proposed changes are to be analysed for potential security threats and their impact on the organisation and their customers.	Functional	Equal	Security Impact Analysis for Changes	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	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 (optional)	Notes (optional)
HSUP30	Asset Lifecycle Security - Information and associated assets	The organisation's information and associated assets are appropriately protected, used, and handled based on their importance.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
HSUP30	Asset Lifecycle Security - Information and associated assets	The organisation's information and associated assets are appropriately protected, used, and handled based on their importance.	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	
HSUP30	Asset Lifecycle Security - Information and associated assets	The organisation's information and associated assets are appropriately protected, used, and handled based on their importance.	Functional	Subset Of	Endpoint Security	END-01	Mechanisms exist to facilitate the implementation of endpoint security controls.	10	
HSUP31	Business Continuity and Disaster Recovery Management - Information security during disruption	In the event of a disruption or failure, critical information or services are identified, and measures are taken for the continuity of services.	Functional	Intersects With	Resume All Missions & Business Functions	BCD-02.1	Mechanisms exist to resume all missions and business functions within Recovery Time Objectives (RTOs) of the contingency plan's activation.	5	
HSUP31	Business Continuity and Disaster Recovery Management - Information security during disruption	In the event of a disruption or failure, critical information or services are identified, and measures are taken for the continuity of services.	Functional	Intersects With	Continue Essential Mission & Business Functions	BCD-02.2	Mechanisms exist to continue essential missions and business functions with little or no loss of operational continuity and sustain that continuity until full system restoration at primary processing and/or storage sites.	5	
HSUP32	Cryptography - Use of cryptography	Rules for effective use of cryptography, including encryption, and key management are defined and implemented.	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	
HSUP33	Identity and Access Management - Identity Management	The complete lifecycle of the account(s) being used to access, process, or manage information and services is managed.	Functional	Equal	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	10	
HSUP34	Identity and Access Management - Information Authentication	User accounts are authenticated and circumventing the authentication process is prevented.	Functional	Equal	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).	10	
HSUP35	Identity and Access Management - Access Rights	Access to information and its associated assets is defined and authorised according to the business, customer and security requirements by adhering to the organisation's identity and access management policy or procedures.	Functional	Intersects With	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	5	
HSUP35	Identity and Access Management - Access Rights	Access to information and its associated assets is defined and authorised according to the business, customer and security requirements by adhering to the organisation's identity and access management policy or procedures.	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	
HSUP36	Identity and Access Management - Privileged Access Rights	Organisations are to ensure that only authorised users, software components and services are provided with privileged access rights.	Functional	Equal	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.	10	
HSUP37	Identity and Access Management - Access to source code	Access to source code, development tools, and software libraries are restricted, appropriately managed, and maintained.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	5	
HSUP37	Identity and Access Management - Access to source code	Access to source code, development tools, and software libraries are restricted, appropriately managed, and maintained.	Functional	Intersects With	Access to Program Source Code	TDA-20	Mechanisms exist to limit privileges to change software resident within software libraries.	5	
HSUP38	Information Security Governance - Performance Measurement	Metrics affecting the organisation's cyber security posture are regularly reported to the Board, and any decisions made are clearly documented.	Functional	Intersects With	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.	5	
HSUP38	Information Security Governance - Performance Measurement	Metrics affecting the organisation's cyber security posture are regularly reported to the Board, and any decisions made are clearly documented.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	5	
HSUP39	Physical and Environmental Security - Maintenance of Physical and Environmental Security	Update, protect and maintain the devices installed as physical security safeguards including the utilities.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
HSUP40	Physical and Environmental Security - Visitor Management System	Secure areas of the organisation are protected from unauthorised personnel.	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	
HSUP40	Physical and Environmental Security - Visitor Management System	Secure areas of the organisation are protected from unauthorised 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	
HSUP41	Remote Working - Remote Working Requirements	Secure mechanisms are available and supported by a documented policy or guidelines to connect to the organisation's or customer's network.	Functional	Intersects With	Identification & Authentication for Third Party Systems & Services	IAC-05	Mechanisms exist to identify and authenticate third-party systems and services.	5	
HSUP41	Remote Working - Remote Working Requirements	Secure mechanisms are available and supported by a documented policy or guidelines to connect to the organisation's or customer's 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	
HSUP42	Web Security - Security of Web Applications	Security controls are implemented if the organisation is developing the web applications to protect them and their customers from potential cyber-attacks.	Functional	Subset Of	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10	
HSUP42	Web Security - Security of Web Applications	Security controls are implemented if the organisation is developing the web applications to protect them and their customers from potential cyber-attacks.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to update products, including systems, software and services, to improve functionality and correct security deficiencies.	5	
HSUP42	Web Security - Security of Web Applications	Security controls are implemented if the organisation is developing the web applications to protect them and their customers from potential cyber-attacks.	Functional	Intersects With	Secure Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.	5	
HSUP43	Cloud Security - Cloud Security Architecture	The organisation's architectural strategy supports the adoption of cloud technologies.	Functional	Equal	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.	10	
HSUP44	Cloud Security - Use of application & programming interface (API)	Organisations are to make use of developed and configured APIs for secure transfer of information between different cloud components.	Functional	Equal	Application & Program Interface (API) Security	CLD-04	Mechanisms exist to ensure support for secure interoperability between components with Application & Program Interfaces (APIs).	10	
HSUP45	Cloud Security - Cloud security controls	Organisations are to ensure that appropriate controls are implemented to protect information in a multi-tenant cloud environment.	Functional	Equal	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.	10	
HSUP46	Communications Security - Network security	Networks and network devices that are used within the organisation are to be securely managed.	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	
HSUP46	Communications Security - Network security	Networks and network devices that are used within the organisation are to be securely managed.	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
HSUP46	Communications Security - Network security	Networks and network devices that are used within the organisation are to be securely managed.	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	
HSUP47	Communications Security - Segregation of networks	The systems and applications that are used to process, store, or transmit information are connected to a separate, dedicated network.	Functional	Intersects With	Isolation of Information System Components	NET-03.7	Mechanisms exist to employ boundary protections to isolate systems, services and processes that support critical missions and/or business functions.	5	
HSUP47	Communications Security - Segregation of networks	The systems and applications that are used to process, store, or transmit information are connected to a separate, dedicated network.	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	5	
HSUP48	Information Backups - Information backup	Backup copies of information, software, services provided, and relevant systems are protected and maintained in accordance with the backup and recovery procedures.	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
HSUP48	Information Backups - Information backup	Backup copies of information, software, services provided, and relevant systems are protected and maintained in accordance with the backup and recovery procedures.	Functional	Intersects With	Backup Modification and/or Destruction	BCD-11.10	Mechanisms exist to restrict access to modify and/or delete backups to privileged users with assigned data backup and recovery operations roles.	5	
HSUP49	Information Backups - Backup restoration	Backups are tested for their restoration in accordance with the documented backup and recovery procedures. Organisations are able to access restored backups as well.	Functional	Equal	Testing for Reliability & Integrity	BCD-11.1	Mechanisms exist to routinely test backups that verify the reliability of the backup process, as well as the integrity and availability of the data.	10	
HSUP50	Change Management - Separate production and non-production environments	Organisations developing inhouse systems, applications, or services are to maintain separate production and non-production environments.	Functional	Equal	Separation of Development, Testing and Operational Environments	TDA-08	Mechanisms exist to manage separate development, testing and operational environments to reduce the risks of unauthorized access or changes to the operational environment and to ensure no impact to production systems.	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 (optional)	Notes (optional)
HSUP51	Patch and Vulnerability Management - Patch and vulnerabilities remediation	Identified vulnerabilities or unpatched systems, services or applications are properly identified, tracked, and remediated.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
HSUP51	Patch and Vulnerability Management - Patch and vulnerabilities remediation	Identified vulnerabilities or unpatched systems, services or applications are properly identified, tracked, and remediated.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
HSUP52	Configuration Management - Secure configuration	Organisations have a standardised baseline configuration in place for new and existing systems, services, and applications.	Functional	Equal	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	10	
HSUP53	Capacity Management - Capacity management	The capacity requirements for maintenance of information processing facilities, communication, and environmental support during contingency operations are met.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
HSUP53	Capacity Management - Capacity management	The capacity requirements for maintenance of information processing facilities, communication, and environmental support during contingency operations are met.	Functional	Subset Of	Capacity & Performance Management	CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	10	
HSUP54	Endpoint Security - Malware protection	Information, services, and applications on organisation systems and associated assets are protected against malware.	Functional	Equal	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	10	
HSUP55	Data Leakage Prevention - Data leakage prevention	Organisations are to detect and prevent data leakage through the unauthorised disclosure and siphoning of information by individuals, systems, or services.	Functional	Intersects With	Monitoring For Information Disclosure	MON-11	Mechanisms exist to monitor for evidence of unauthorized exfiltration or disclosure of non-public information.	5	
HSUP55	Data Leakage Prevention - Data leakage prevention	Organisations are to detect and prevent data leakage through the unauthorised disclosure and siphoning of information by individuals, systems, or services.	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	
HSUP56	Business Continuity and Disaster Recovery Management - ICT readiness for business continuity	The lessons learned from business continuity and disaster recovery testing are reflected in the established and implemented information security controls.	Functional	Equal	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-05	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	10	
HSUP57	Physical and Environmental Security - Monitoring of physical and environmental security mechanisms	Installed physical and environmental security mechanisms are monitored for potential security incidents.	Functional	Equal	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	10	
HSUP58	Compliance - Review of compliance requirements	Regular reviews are performed to confirm that the legal, regulatory, statutory, and contractual requirements are met.	Functional	Intersects With	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's executive leadership.	5	
HSUP58	Compliance - Review of compliance requirements	Regular reviews are performed to confirm that the legal, regulatory, statutory, and contractual requirements are met.	Functional	Intersects With	Internal Audit Function	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.	5	
HSUP58	Compliance - Review of compliance requirements	Regular reviews are performed to confirm that the legal, regulatory, statutory, and contractual requirements are met.	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
HSUP59	Systems Acquisition, Development and Maintenance - Independent reviews	Independent security reviews are defined and implemented before any new or major upgrades on systems are moved to the production environment.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy assessment and authorization controls.	10	
HSUP59	Systems Acquisition, Development and Maintenance - Independent reviews	Independent security reviews are defined and implemented before any new or major upgrades on systems are moved to the production environment.	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the cybersecurity & data privacy controls in systems, applications and services through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5	
HSUP60	Information Backups - Monitoring of backups	Authorised personnel or teams are alerted upon unsuccessful backups.	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
HSUP60	Information Backups - Monitoring of backups	Authorised personnel or teams are alerted upon unsuccessful backups.	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	
HSUP60	Information Backups - Monitoring of backups	Authorised personnel or teams are alerted upon unsuccessful backups.	Functional	Intersects With	Automated Alerts	MON-01.12	Mechanisms exist to automatically alert incident response personnel to inappropriate or anomalous activities that have potential security incident implications.	5	
HSUP60	Information Backups - Monitoring of backups	Authorised personnel or teams are alerted upon unsuccessful backups.	Functional	Intersects With	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data privacy and supply chain activities to achieve integrated situational awareness.	5	
HSUP61	Logging and Monitoring - Logging and monitoring	The activities performed on the information processing systems, services, and applications are logged and stored as per the organisation's (and the customer's) logging and auditing requirements.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
HSUP61	Logging and Monitoring - Logging and monitoring	The activities performed on the information processing systems, services, and applications are logged and stored as per the organisation's (and the customer's) logging and auditing requirements.	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure systems to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5	
HSUP61	Logging and Monitoring - Logging and monitoring	The activities performed on the information processing systems, services, and applications are logged and stored as per the organisation's (and the customer's) logging and auditing requirements.	Functional	Intersects With	Audit Trails	MON-03.2	Mechanisms exist to link system access to individual users or service accounts.	5	
HSUP62	Logging and Monitoring - Clock synchronisation	The information processing systems, applications, devices, and services are synchronised to an approved time source.	Functional	Equal	Synchronization With Authoritative Time Source	MON-07.1	Mechanisms exist to synchronize internal system clocks with an authoritative time source.	10	
HSUP63	Human Resource Security - Terms and conditions of employment	Breach of employment and supplier agreements are enforced.	Functional	Intersects With	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	5	
HSUP63	Human Resource Security - Terms and conditions of employment	Breach of employment and supplier agreements are enforced.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
HSUP64	Asset Lifecycle Security - Information and associated assets	Misuse of the organisation's assets is investigated, and documented procedures are followed as stated in the acceptable use policy, contractor agreements, or service agreements.	Functional	Intersects With	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	5	
HSUP64	Asset Lifecycle Security - Information and associated assets	Misuse of the organisation's assets is investigated, and documented procedures are followed as stated in the acceptable use policy, contractor agreements, or service agreements.	Functional	Intersects With	Workplace Investigations	HRS-07.1	Mechanisms exist to conduct employee misconduct investigations when there is reasonable assurance that a policy has been violated.	5	
HSUP64	Asset Lifecycle Security - Information and associated assets	Misuse of the organisation's assets is investigated, and documented procedures are followed as stated in the acceptable use policy, contractor agreements, or service agreements.	Functional	Intersects With	Monitoring for Third-Party Information Disclosure	TPM-07	Mechanisms exist to monitor for evidence of unauthorized exfiltration or disclosure of organizational information.	5	
HSUP64	Asset Lifecycle Security - Information and associated assets	Misuse of the organisation's assets is investigated, and documented procedures are followed as stated in the acceptable use policy, contractor agreements, or service agreements.	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity & data privacy controls.	5	
HML01	Information security policy - Policies for information security	A clear information security policy, acceptable use policy, topic-specific policies and procedures are in place to maintain information security.	Functional	Equal	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	10	
HSUP65	Information Security Incident Management - Learning from information security incident	Organisations report all security incidents and near misses to their senior management or to the Board by a nominated Information Security Officer. All customer-related incidents are to be notified to the customer as per agreed timelines.	Functional	Intersects With	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.	5	
HSUP65	Information Security Incident Management - Learning from information security incident	Organisations report all security incidents and near misses to their senior management or to the Board by a nominated Information Security Officer. All customer-related incidents are to be notified to the customer as per agreed timelines.	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	
HSUP66	Information Security Incident Management - Collection of evidence	Evidence gathered as part of the incident management process is appropriately protected.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	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 (optional)	Notes (optional)
HSUP66	Information Security Incident Management - Collection of evidence	Evidence gathered as part of the incident management process is appropriately protected.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is stored.	5	
HSUP66	Information Security Incident Management - Collection of evidence	Evidence gathered as part of the incident management process is appropriately protected.	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	