

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

Reference document: Secure Controls Framework (SCF) version 2026.1
 https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document:

Focal Document URL: <https://www.tewhaturora.govt.nz/publications/health-information-security-framework/>
 Published STRM URL: <https://content.securecontrolsframework.com/strm/scf-strm-apac-nz-hisf-microsmall-2023.pdf>

HISO 10029:2025 NZ Health Information Security Framework (HISF) - MLHSP (2023)

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
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 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	
HHSP01	Information security policy - Policies for information security	A clear information security policy, acceptable use policy and topic-specific policies and procedures are in place.	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	
HHSP02	Human resource security - Terms and conditions of employment	Hospitals processing and storing health information include the security roles and responsibilities of personnel within job descriptions.	Functional	Equal	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
HHSP03	Human resource security - Terms and conditions of employment	A breach of information security, including health 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	
HHSP03	Human resource security - Terms and conditions of employment	A breach of information security, including health 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	
HHSP04	Human resource security - Onboarding, offboarding and role change	Procedures for providing and revoking logical and physical access when personnel join, have a role change, or leave the hospital are in place.	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	
HHSP04	Human resource security - Onboarding, offboarding and role change	Procedures for providing and revoking logical and physical access when personnel join, have a role change, or leave the hospital are in place.	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	
HHSP04	Human resource security - Onboarding, offboarding and role change	Procedures for providing and revoking logical and physical access when personnel join, have a role change, or leave the hospital are in place.	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	
HHSP04	Human resource security - Onboarding, offboarding and role change	Procedures for providing and revoking logical and physical access when personnel join, have a role change, or leave the hospital are in place.	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	
HHSP05	Asset lifecycle security - Health information and associated assets	Asset management process(es) is 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	
HHSP06	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	
HHSP07	Health information security incident management - Planning and preparation	A health 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	
HHSP07	Health information security incident management - Planning and preparation	A health 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	
HHSP08	Business continuity and disaster recovery management - Information security during disruption	Documented, approved, business continuity and disaster recovery management, operational resilience policies and procedures are established.	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 (BCDR) playbooks).	10	
HHSP09	Supplier management - Policy for suppliers	The information security requirements for managing the risks while a supplier is accessing health information are identified and communicated.	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	
HHSP10	Identity and access management - Access control	Establish, document, approve, and implement rules to control physical and logical access to health 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	
HHSP10	Identity and access management - Access control	Establish, document, approve, and implement rules to control physical and logical access to health information and its assets.	Functional	Intersects With	Access To Critical Systems	PES-03.4	Physical access control mechanisms exist to enforce physical access to critical systems or sensitive/regulate data, in addition to the physical access controls for the facility.	5	
HHSP11	Medical devices - Purchase or lease	Hospitals are to include cyber security in procurement planning and decisions.	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 each Technology Asset, Application and/or Service (TAAS) under their control.	5	
HHSP11	Medical devices - Purchase or lease	Hospitals are to include cyber security in procurement planning and decisions.	Functional	Intersects With	Security, Compliance & Resilience in Project Management	PRM-04	Mechanisms exist to assess security, compliance and resilience 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	
HHSP11	Medical devices - Purchase or lease	Hospitals are to include cyber security in procurement planning and decisions.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
HHSP12	Information Security Governance - Ownership of information security	The Board is accountable for hospitals information security governance.	Functional	Equal	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.	10	
HHSP13	Physical and environmental security - Policies and procedures	A documented policy and supporting procedures for maintaining physical security within the hospital is in place.	Functional	Equal	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.	10	
HHSP14	Physical and environmental security - Clear desk and clear screen policy	A documented and approved procedure to remove papers and removable storage from easily accessible areas is implemented.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
HHSP14	Physical and environmental security - Clear desk and clear screen policy	A documented and approved procedure to remove papers and removable storage from easily accessible areas is implemented.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulate data wherever it is processed and/or stored.	5	
HHSP14	Physical and environmental security - Clear desk and clear screen policy	A documented and approved procedure to remove papers and removable storage from easily accessible areas is 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	
HHSP15	Cloud security - Cloud security policy & cloud security agreement (CSA)	Hospitals have planned maintenance of health information via cloud services as documented in 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	
HHSP16	System acquisition, development and maintenance - Security while developing applications, products or services	Health information systems are securely designed, and appropriate controls are implemented.	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 each Technology Asset, Application and/or Service (TAAS) under their control.	5	
HHSP16	System acquisition, development and maintenance - Security while developing applications, products or services	Health 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 security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	
HHSP17	Information backups - Policies 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 satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
HHSP17	Information backups - Policies and procedures	A backup and recovery procedure is in place.	Functional	Intersects With	Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.	5	
HHSP18	Change Management - Policies and procedures	A documented process is in place for performing changes to new and existing systems or services related to health information.	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
HHSP18	Change Management - Policies and procedures	A documented process is in place for performing changes to new and existing systems or services related to health information.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
HHSP19	Patch and vulnerability management - Policies and procedures	A documented process is in place for identifying vulnerabilities and updating patches on the hospital's systems, services and applications.	Functional	Subset Of	Vulnerability & Patch Management Program (VPM)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
HHSP19	Patch and vulnerability management - Policies and procedures	A documented process is in place for identifying vulnerabilities and updating patches on the hospital's systems, services and applications.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
HHSP19	Patch and vulnerability management - Policies and procedures	A documented process is in place for identifying vulnerabilities and updating patches on the hospital's systems, services and applications.	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	
HHSP20	Human resource security - Terms and conditions of employment	Hospitals, at a minimum, screen all personnel by verifying their identity, previous employment, applicable health 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	
HHSP21	Human resource security - Roles and responsibilities	Hospitals processing health information are to ensure: a: information security responsibilities are clearly defined and assigned to a governance body overseeing health information security activities is in place c: at least one individual is responsible for health information security.	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 (SCR).	5	
HHSP21	Human resource security - Roles and responsibilities	Hospitals processing health information are to ensure: a: information security responsibilities are clearly defined and assigned to a governance body overseeing health information security activities is in place c: at least one individual is responsible for health information security.	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 managing, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
HHSP21	Human resource security - Roles and responsibilities	Hospitals processing health information are to ensure: a: information security responsibilities are clearly defined and assigned to a governance body overseeing health information security activities is in place c: at least one individual is responsible for health information security.	Functional	Intersects With	Authoritative Chain of Command	GOV-04.2	Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
HHSP22	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	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness 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	Notes
HHS23	Health information security incident management - Roles and responsibilities	Hospitals processing and storing health information have roles and responsibilities determined for carrying out the incident management process.	Functional	Equal	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
HHS24	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 impacts and risk to hospitals.	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	
HHS24	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 impacts and risk to hospitals.	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	
HHS25	Supplier management - Supply chain risks	Suppliers are systematically evaluated, and their information security activities are reviewed before and after onboarding of their systems and services.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
HHS25	Supplier management - Supply chain risks	Suppliers are systematically evaluated, and their information security activities are reviewed before and after onboarding of their systems and services.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5	
HHS25	Supplier management - Supply chain risks	Suppliers are systematically evaluated, and their information security activities are reviewed before and after onboarding of their systems and services.	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 security, compliance and resilience controls.	5	
HHS26	Medical devices - Medical device scanning	Vulnerability scanning on medical devices is only performed when they are in a test environment not connected for patient care.	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
HHS26	Medical devices - Medical device scanning	Vulnerability scanning on medical devices is only performed when they are in a test environment not connected for patient care.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMPP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability scanning of systems and applications.	10	
HHS26	Medical devices - Medical device scanning	Vulnerability scanning on medical devices is only performed when they are in a test environment not connected for patient care.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
HHS27	Information Security Governance - Roles and responsibilities	Roles and responsibilities are defined and documented for planning, implementing, operating, assessing, and reporting on the hospitals information security requirements.	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 (SCRPP).	5	
HHS27	Information Security Governance - Roles and responsibilities	Roles and responsibilities are defined and documented for planning, implementing, operating, assessing, and reporting on the hospitals 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 Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
HHS28	Information Security Governance - Information security in project management	Hospitals are to integrate information security into project management.	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 each Technology Asset, Application and/or Service (TAAS) under their control.	5	
HHS28	Information Security Governance - Information security in project management	Hospitals are to integrate information security into project management.	Functional	Intersects With	Security, Compliance & Resilience in Project Management	PRM-04	Mechanisms exist to assess security, compliance and resilience 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	
HHS28	Information Security Governance - Information security in project management	Hospitals are to integrate information security into project management.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
HHS29	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	
HHS30	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	
HHS31	System acquisition, development and maintenance - Business and security requirements	Health information business security requirements are identified, documented and approved when developing or acquiring applications.	Functional	Intersects With	Security, Compliance & Resilience in Project Management	PRM-04	Mechanisms exist to assess security, compliance and resilience 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	
HHS31	System acquisition, development and maintenance - Business and security requirements	Health information business security requirements are identified, documented and approved when developing or acquiring applications.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
HHS31	System acquisition, development and maintenance - Business and security requirements	Health information business security requirements are identified, documented and approved when developing or acquiring applications.	Functional	Intersects With	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	5	
HHS32	Risk management - Risk assessments	Risk assessments are performed on new and existing systems and applications that manage health information to understand and manage the risks posed to the hospital 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 Technology Assets, Applications, Services and/or Data (TAASD).	10	
HHS33	Change Management - Security testing	The proposed changes are to be analysed for potential security threats and their impact to the hospital.	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	
HHS34	Asset lifecycle security - Health information and associated assets	Health 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	
HHS34	Asset lifecycle security - Health information and associated assets	Health information and associated assets are appropriately protected, used, and handled based on their importance.	Functional	Subset Of	Endpoint Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	10	
HHS35	Business continuity and disaster recovery management - Information security during disruption	In the event of a disruption or failure, critical health information and/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	
HHS35	Business continuity and disaster recovery management - Information security during disruption	In the event of a disruption or failure, critical health information and/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	
HHS36	Supplier management - Information security within supplier agreements	The hospitals information security requirements are to be included in the agreements with the suppliers.	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	
HHS37	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	
HHS38	Identity and access management - Identity management	The complete lifecycle of user account(s) being used to access, process, or manage health information 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	
HHS39	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	
HHS40	Identity and access management - Access rights	Access to health information and its associated assets is defined and authorised according to the business and security requirements and adhere to the hospitals identity and access management policy or procedures.	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	
HHS40	Identity and access management - Access rights	Access to health information and its associated assets is defined and authorised according to the business and security requirements and adhere to the hospitals identity and access management policy or procedures.	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	
HHS41	Identity and access management - Privileged access rights	Hospitals 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 Technology Assets, Applications and/or Services (TAAS).	10	
HHS42	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 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	
HHS42	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	
HHS43	Medical devices - Protecting medical devices	Where possible, production and legacy medical devices are on a separate network.	Functional	Intersects With	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.	5	
HHS43	Medical devices - Protecting medical devices	Where possible, production and legacy medical devices are on a separate network.	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
HHS43	Medical devices - Protecting medical devices	Where possible, production and legacy medical devices are on a separate network.	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 missions/business needs.	5	
HHS44	Medical devices - Maintenance	All medical devices are maintained as per the latest updates from the manufacturers and current industry/regulatory standards.	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	
HHS45	Medical devices - Dispose or return lease	Medical devices with patient health information are digitally sanitised before their disposal or when they are being returned.	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	
HHS46	Information Security Governance - Performance measurement	Metrics affecting the hospitals 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 Security, Compliance & Resilience Program (SCRPP).	5	
HHS46	Information Security Governance - Performance measurement	Metrics affecting the hospitals 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 Security, Compliance & Resilience Program (SCRPP) measures of performance.	5	
HHS47	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	
HHS48	Physical and environmental security - Visitor management system	Secure areas of the hospital 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	

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
HHSF48	Physical and environmental security - Visitor management system	Secure areas of the hospital are protected from unauthorised personnel.	Functional	Intersects With	Physical Security of Offices, Rooms & Facilities	PE5-04	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	
HHSF49	Remote working - Remote working requirements	Secure mechanisms are available and supported by a documented policy or guidelines to connect to the hospital network and access health information.	Functional	Intersects With	Identification & Authentication for Third-Party Technology Assets, Applications and/or Services (TAAS)	IAC-05	Mechanisms exist to identify and authenticate third-party Technology Assets, Applications and/or Services (TAAS).	5	
HHSF49	Remote working - Remote working requirements	Secure mechanisms are available and supported by a documented policy or guidelines to connect to the hospital network and access health information.	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	
HHSF50	Web security - Security of web applications	Security controls are implemented while developing the web applications to protect hospitals 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	
HHSF50	Web security - Security of web applications	Security controls are implemented while developing the web applications to protect hospitals from potential cyber-attacks.	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	
HHSF50	Web security - Security of web applications	Security controls are implemented while developing the web applications to protect hospitals from potential cyber-attacks.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5	
HHSF51	Cloud security - Cloud security architecture	The hospital'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	
HHSF52	Cloud security - Use of application & programming interface (API)	Hospitals are to make use of developed and configured APIs for secure transfer of health information between different cloud components.	Functional	Equal	Application Programming Interface (API) Security	CLD-04	Mechanisms exist to ensure support for secure interoperability between components with Application Programming Interfaces (APIs).	10	
HHSF53	Cloud security - Cloud security controls	Hospitals are to ensure that appropriate controls are implemented to protect health 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 defined and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	10	
HHSF54	Communications security - Network security	Networks and network devices used within hospitals or supporting hospitals systems and applications are 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	
HHSF54	Communications security - Network security	Networks and network devices used within hospitals or supporting hospitals systems and applications are securely managed.	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	
HHSF54	Communications security - Network security	Networks and network devices used within hospitals or supporting hospitals systems and applications are 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	
HHSF55	Communications security - Segregation of networks	The systems and applications used to process, store or transmit health information are connected to a separate, dedicated network.	Functional	Intersects With	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.	5	
HHSF55	Communications security - Segregation of networks	The systems and applications used to process, store or transmit health information are connected to a separate, dedicated network.	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.	5	
HHSF56	Information backups - Information backup	Backup copies of health information, software and systems are protected and maintained in accordance with the backup and recovery procedures.	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	
HHSF56	Information backups - Information backup	Backup copies of health information, software and 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 satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
HHSF56	Information backups - Information backup	Backup copies of health information, software and 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 satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
HHSF56	Information backups - Information backup	Backup copies of health information, software and 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	
HHSF57	Information backups - Backup restoration	Health information backups are tested for their restoration in accordance with the documented backup and recovery procedures. Hospitals 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	
HHSF58	Change Management - Separate production and non-production environments	Hospitals developing in-house systems and applications 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 Technology Assets, Applications and/or Services (TAAS).	10	
HHSF59	Patch and vulnerability management - Patch and vulnerabilities remediation	Identified vulnerabilities or unpatched systems, services or applications within the hospital 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	
HHSF59	Patch and vulnerability management - Patch and vulnerabilities remediation	Identified vulnerabilities or unpatched systems, services or applications within the hospital 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	
HHSF60	Configuration management - Secure configuration	Hospitals have a standardised baseline configuration in place for new and existing operating systems, services and applications.	Functional	Equal	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.	10	
HHSF61	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 Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
HHSF61	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	
HHSF62	Endpoint security - Malware protection	Health information on hospital systems and associated assets are protected against malware.	Functional	Equal	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize anti-malware technologies to detect and eradicate malicious code.	10	
HHSF63	Data leakage prevention - Data leakage prevention	Hospitals 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	
HHSF63	Data leakage prevention - Data leakage prevention	Hospitals 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	
HHSF64	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	
HHSF65	Medical devices - Compliance activities	Medical devices are compliant with relevant standards, and the identified risks are documented within the medical device risk register.	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	
HHSF65	Medical devices - Compliance activities	Medical devices are compliant with relevant standards, and the identified risks are documented within the medical device risk register.	Functional	Intersects With	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	
HHSF65	Medical devices - Compliance activities	Medical devices are compliant with relevant standards, and the identified risks are documented within the medical device risk register.	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
HHSF66	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	PE5-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	10	
HHSF67	Compliance - Review of compliance requirements	Regular reviews are performed to confirm that the legal, regulatory, statutory, and contractual requirements are met.	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	
HHSF67	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	
HHSF67	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 Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRPR), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
HHSF68	System 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 security, compliance and resilience assessment and authorization controls.	10	
HHSF68	System 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 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	
HHSF69	Information backups - Monitoring of backups	Authorised personnel or teams are alerted upon unsuccessful or incomplete 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 satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
HHSF69	Information backups - Monitoring of backups	Authorised personnel or teams are alerted upon unsuccessful or incomplete 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	
HHSF69	Information backups - Monitoring of backups	Authorised personnel or teams are alerted upon unsuccessful or incomplete 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	
HHSF69	Information backups - Monitoring of backups	Authorised personnel or teams are alerted upon unsuccessful or incomplete backups.	Functional	Intersects With	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	5	
HHSF70	Logging and monitoring - Logging and monitoring	The activities performed on the health information processing systems, services and applications are logged and stored as per the hospitals logging and auditing requirements.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring 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	Notes
HHSF70	Logging and monitoring - Logging and monitoring	The activities performed on the health information processing systems, services and applications are logged and stored as per the hospitals logging and auditing requirements.	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	
HHSF70	Logging and monitoring - Logging and monitoring	The activities performed on the health information processing systems, services and applications are logged and stored as per the hospitals 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	
HHSF71	Logging and monitoring - Clock synchronisation	The health information processing systems, services and applications 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	
HHSF72	Human resource security - Terms and conditions of employment	Breach of employment agreements 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	
HHSF72	Human resource security - Terms and conditions of employment	Breach of employment agreements and supplier agreements are enforced.	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	
HHSF73	Asset lifecycle security - Health information and associated assets	Misuse of the hospital'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	
HHSF73	Asset lifecycle security - Health information and associated assets	Misuse of the hospital'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	
HHSF73	Asset lifecycle security - Health information and associated assets	Misuse of the hospital'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	
HHSF73	Asset lifecycle security - Health information and associated assets	Misuse of the hospital'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 security, compliance and resilience controls.	5	
HHSF74	Health information security incident management - Collection of evidence	Evidence gathered as part of the health incident management process is appropriately protected.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
HHSF74	Health information security incident management - Collection of evidence	Evidence gathered as part of the health 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 processed and/or stored.	5	
HHSF74	Health information security incident management - Collection of evidence	Evidence gathered as part of the health 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	
HHSF75	Health information security incident management - Learning from a health information security incident	Hospitals report all security incidents and near misses to the hospital's senior management or to the Board by a nominated Information Security Officer.	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 Security, Compliance & Resilience Program (SCRCP).	5	
HHSF75	Health information security incident management - Learning from a health information security incident	Hospitals report all security incidents and near misses to the hospital's senior management or to the Board by a nominated Information Security Officer.	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	
HML02	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	
HML02	Human resource security - Terms and conditions of employment	Security roles and responsibilities of personnel are included within job descriptions.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
HML03	Human resource security - Terms and conditions of employment	A breach of information security, including 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	
HML03	Human resource security - Terms and conditions of employment	A breach of information security, including 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	
HML04	Human resource security - Onboarding, offboarding and role change	Procedures for providing and revoking logical and physical access when personnel join, have a role change or leave the organisation are in place.	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	
HML04	Human resource security - Onboarding, offboarding and role change	Procedures for providing and revoking logical and physical access when personnel join, have a role change or leave the organisation are in place.	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	
HML04	Human resource security - Onboarding, offboarding and role change	Procedures for providing and revoking logical and physical access when personnel join, have a role change or leave the organisation are in place.	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	
HML04	Human resource security - Onboarding, offboarding and role change	Procedures for providing and revoking logical and physical access when personnel join, have a role change or leave the organisation are in place.	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	
HML05	Asset lifecycle security - Information and associated assets	Asset management process(es) is 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	
HML06	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	
HML07	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	
HML07	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	
HML08	Business continuity and disaster recovery management - Information security during disruption	Documented, approved, business continuity and disaster recovery management, operational resilience policies and procedures are established.	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	
HML09	Supplier management - Policy for suppliers	The information security requirements for managing the risks while a supplier is accessing information are to be identified and communicated.	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	
HML10	Identify 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	
HML10	Identify 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 Critical Systems	PES-03.4	Physical access control mechanisms exist to enforce physical access to critical systems or sensitive/regulated data, in addition to the physical access controls for the facility.	5	
HML11	Medical devices - Purchase or lease	Organisations are to include cyber security in procurement planning and decisions.	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 each Technology Asset, Application and/or Service (TAAS) under their control.	5	
HML11	Medical devices - Purchase or lease	Organisations are to include cyber security in procurement planning and decisions.	Functional	Intersects With	Security, Compliance & Resilience in Project Management	PRM-04	Mechanisms exist to assess security, compliance and resilience 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	
HML12	Information security governance - Ownership of information security	The organisation's Board or information security steering committee is accountable for organisations information security governance.	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	
HML12	Information security governance - Ownership of information security	The organisation's Board or information security steering committee is accountable for organisations 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 Security, Compliance & Resilience Program (SCRCP).	5	
HML13	Physical and environmental security - Policies and procedures	A documented policy and supporting procedures for maintaining physical security within the organisation is in place.	Functional	Equal	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.	10	
HML14	Physical and environmental security - Clear desk and clear screen policy	A documented and approved procedure to remove papers and removable storage from easily accessible areas is implemented.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
HML14	Physical and environmental security - Clear desk and clear screen policy	A documented and approved procedure to remove papers and removable storage from easily accessible areas is implemented.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.	5	
HML14	Physical and environmental security - Clear desk and clear screen policy	A documented and approved procedure to remove papers and removable storage from easily accessible areas is 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	
HML15	Cloud security - Cloud security policy & cloud security agreement (CSA)	Organisations have planned maintenance of information 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	

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
HML16	System acquisition, development and maintenance - Security while developing applications, products or services	Information systems are securely designed, and appropriate controls are implemented.	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	
HML16	System 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 Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for each Technology Asset, Application and/or Service (TAAS) under their control.	5	
HML16	System 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 security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	
HML17	Information backups - Policies 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 satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
HML17	Information backups - Policies and procedures	A backup and recovery procedure is in place.	Functional	Intersects With	Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstruction	BCD-12	Mechanisms exist to ensure the secure recovery and reconstruction of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.	5	
HML18	Change management - Policies and procedures	A documented process is in place for performing changes to new and existing systems or services related to information.	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
HML18	Change management - Policies and procedures	A documented process is in place for performing changes to new and existing systems or services related to information.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
HML19	Patch and vulnerability management - Policies and procedures	A documented process is in place for identifying vulnerabilities and updating patches on the organisations systems, applications, tools, services etc.	Functional	Subset Of	Vulnerability & Patch Management Program (VPM)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
HML19	Patch and vulnerability management - Policies and procedures	A documented process is in place for identifying vulnerabilities and updating patches on the organisations 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	
HML19	Patch and vulnerability management - Policies and procedures	A documented process is in place for identifying vulnerabilities and updating patches on the organisations systems, applications, tools, services etc.	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	
HML20	Human resource security - Terms and conditions of employment	Organisations, at a minimum, screen all personnel by verifying their identity, previous employment, applicable health 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	
HML21	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 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	
HML21	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 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 (SCR).	5	
HML21	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 Technology Assets, Applications, Services and/or Data (TAAS)-related risks.	5	
HML22	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	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
HML23	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	
HML24	Business continuity and disaster recovery management - ICT readiness for business continuity	Establish criteria for developing business continuity, disaster recovery, operational resilience strategies, and capabilities are to be determined 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 Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
HML24	Business continuity and disaster recovery management - ICT readiness for business continuity	Establish criteria for developing business continuity, disaster recovery, operational resilience strategies, and capabilities are to be determined 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	
HML25	Supplier management - Supply chain risks	Suppliers are to be systematically evaluated, and their information security activities are reviewed before and after onboarding of their systems and services.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
HML25	Supplier management - Supply chain risks	Suppliers are to be systematically evaluated, and their information security activities are reviewed before and after onboarding of their systems and services.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5	
HML25	Supplier management - Supply chain risks	Suppliers are to be systematically evaluated, and their information security activities are reviewed before and after onboarding of their systems and services.	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 security, compliance and resilience controls.	5	
HML26	Medical devices - Medical device scanning	Vulnerability scanning on medical devices is only performed when they are in a test environment not connected for patient care.	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
HML26	Medical devices - Medical device scanning	Vulnerability scanning on medical devices is only performed when they are in a test environment not connected for patient care.	Functional	Subset Of	Vulnerability & Patch Management Program (VPM)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
HML26	Medical devices - Medical device scanning	Vulnerability scanning on medical devices is only performed when they are in a test environment not connected for patient care.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scans of systems and applications.	5	
HML27	Information security governance - Roles and responsibilities	Roles and responsibilities are defined and documented for planning, implementing, operating, assessing, and reporting on the organisations information security requirements.	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 (SCR).	5	
HML27	Information security governance - Roles and responsibilities	Roles and responsibilities are defined and documented for planning, implementing, operating, assessing, and reporting on the organisations 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 Technology Assets, Applications, Services and/or Data (TAAS)-related risks.	5	
HML28	Information security governance - Information security in project management	Organisations are to integrate information security into project management.	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 each Technology Asset, Application and/or Service (TAAS) under their control.	5	
HML28	Information security governance - Information security in project management	Organisations are to integrate information security into project management.	Functional	Intersects With	Security, Compliance & Resilience in Project Management	PRM-04	Mechanisms exist to assess security, compliance and resilience 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	
HML29	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	
HML30	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	
HML31	System acquisition, development and maintenance - Business and security requirements	Business and security requirements are identified, documented and approved when developing or acquiring applications.	Functional	Intersects With	Security, Compliance & Resilience in Project Management	PRM-04	Mechanisms exist to assess security, compliance and resilience 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	
HML31	System acquisition, development and maintenance - Business and security requirements	Business and security requirements are identified, documented and approved when developing or acquiring applications.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
HML31	System acquisition, development and maintenance - Business and security requirements	Business and security requirements are identified, documented and approved when developing or acquiring applications.	Functional	Intersects With	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	5	
HML32	Risk management - Risk assessments	Risk assessments are performed on new and existing systems and applications that manage information 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 Technology Assets, Applications, Services and/or Data (TAAS).	10	
HML33	Change management - Security testing	The proposed changes are to be analysed for potential security threats and their impact on the organisation.	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	
HML34	Asset lifecycle security - Information and associated assets	Information and associated assets are appropriately protected, used, and handled based on their importance.	Functional	Equal	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	10	
HML35	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	
HML35	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	
HML36	Supplier management - Information security within supplier agreements	The organisation's information security requirements are to be included in the agreements with the suppliers.	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 (TAAS).	10	
HML37	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	
HML38	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	
HML39	Identity and access management - Informative 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	

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
HML40	Identity and access management - Access rights	Access to information and its associated assets is defined and authorised according to the business and security requirements and adhere to the organisation's identity and access management policy or procedures.	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	
HML40	Identity and access management - Access rights	Access to information and its associated assets is defined and authorised according to the business and security requirements and adhere to the organisation's identity and access management policy or procedures.	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	
HML41	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 Technology Assets, Applications and/or Services (TAAS).	10	
HML42	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 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	
HML42	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	
HML43	Medical devices - Protecting medical devices	Where possible, production and legacy medical devices are on a separate network.	Functional	Intersects With	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.	5	
HML43	Medical devices - Protecting medical devices	Where possible, production and legacy medical devices are on a separate network.	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
HML43	Medical devices - Protecting medical devices	Where possible, production and legacy medical devices are on a separate network.	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	
HML44	Medical devices - Maintenance	All medical devices are maintained as per the latest updates from the manufacturers and current industry/regulatory standards.	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	
HML45	Medical devices - Dispose or return lease	Medical devices with patient information are digitally sanitised before their disposal or when they are being returned.	Functional	Equal	Secure Disposal, Destruction and/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	
HML46	Information security governance - Performance measurement	Metrics affecting the organisations 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 security, Compliance & Resilience Program (SCRCP).	5	
HML46	Information security governance - Performance measurement	Metrics affecting the organisations 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 Security, Compliance & Resilience Program (SCRCP) measures of performance.	5	
HML47	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	
HML48	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	
HML48	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	
HML49	Remote working - Remote working requirements	Secure mechanisms are available and supported by a documented policy or guidelines to connect to the organisations network.	Functional	Intersects With	Identification & Authentication for Third-Party Technology Assets, Applications and/or Services (TAAS)	IAC-05	Mechanisms exist to identify and authenticate third-party Technology Assets, Applications and/or Services (TAAS).	5	
HML49	Remote working - Remote working requirements	Secure mechanisms are available and supported by a documented policy or guidelines to connect to the organisations 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	
HML50	Web security - Security of web applications	Security controls are implemented if the organisation is developing the web applications to protect them 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	
HML50	Web security - Security of web applications	Security controls are implemented if the organisation is developing the web applications to protect them from potential cyber-attacks.	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	
HML50	Web security - Security of web applications	Security controls are implemented if the organisation is developing the web applications to protect them from potential cyber-attacks.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5	
HML51	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	
HML52	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 Programming Interface (API) Security	CLD-04	Mechanisms exist to ensure support for secure interoperability between components with Application Programming Interfaces (APIs).	10	
HML53	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	
HML54	Communications security - Network security	Networks and network devices supporting the organisations systems and applications 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	
HML54	Communications security - Network security	Networks and network devices supporting the organisations systems and applications are to be securely managed.	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	
HML54	Communications security - Network security	Networks and network devices supporting the organisations systems and applications 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	
HML55	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 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.	5	
HML55	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 (macrosegmentation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.	5	
HML56	Information backups - Information backup	Backup copies of information, software 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 satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
HML56	Information backups - Information backup	Backup copies of information, software 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 operations to privileged users with assigned data backup and recovery roles.	5	
HML57	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.	5	
HML58	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 Technology Assets, Applications and/or Services (TAAS).	10	
HML59	Patch and vulnerability management - Patch and vulnerabilities remediation	Identified vulnerabilities or unpatched systems, services or applications within the organisation 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	
HML59	Patch and vulnerability management - Patch and vulnerabilities remediation	Identified vulnerabilities or unpatched systems, services or applications within the organisation 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	
HML60	Configuration management - Secure configuration	Organisations have a standardised baseline configuration in place for new and existing systems, services and applications.	Functional	Equal	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.	10	
HML61	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 Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
HML61	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	
HML62	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 antim malware technologies to detect and eradicate malicious code.	10	
HML63	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	
HML64	Medical devices - Compliance activities	Medical devices are compliant with relevant standards, and the identified risks are documented within the medical device risk register.	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	
HML64	Medical devices - Compliance activities	Medical devices are compliant with relevant standards, and the identified risks are documented within the medical device risk register.	Functional	Intersects With	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	
HML64	Medical devices - Compliance activities	Medical devices are compliant with relevant standards, and the identified risks are documented within the medical device risk register.	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
HML65	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	

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
HML66	Compliance - Review of compliance requirements	Regular reviews are performed to confirm that the legal, regulatory, statutory, and contractual requirements are met.	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	
HML66	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	
HML66	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 Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRIP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
HML67	System 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 security, compliance and resilience assessment and authorization controls.	10	
HML67	System 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 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	
HML68	Information backups - Monitoring of backups	Authorised personnel or teams are alerted upon unsuccessful or incomplete 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 satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
HML68	Information backups - Monitoring of backups	Authorised personnel or teams are alerted upon unsuccessful or incomplete 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	
HML68	Information backups - Monitoring of backups	Authorised personnel or teams are alerted upon unsuccessful or incomplete 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	
HML68	Information backups - Monitoring of backups	Authorised personnel or teams are alerted upon unsuccessful or incomplete backups.	Functional	Intersects With	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	5	
HML69	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	
HML69	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	
HML70	Logging and monitoring - Logging and monitoring	The activities performed on the information processing systems, services and applications are logged and stored as per the organisations logging and auditing requirements.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
HML70	Logging and monitoring - Logging and monitoring	The activities performed on the information processing systems, services and applications are logged and stored as per the organisations logging and auditing requirements.	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	
HML70	Logging and monitoring - Logging and monitoring	The activities performed on the information processing systems, services and applications are logged and stored as per the organisations 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	
HML71	Logging and monitoring - Clock synchronisation	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	
HML72	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	
HML72	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 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	
HML73	Asset lifecycle security - Information and associated assets	Misuse of the organisations 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	
HML73	Asset lifecycle security - Information and associated assets	Misuse of the organisations 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	
HML73	Asset lifecycle security - Information and associated assets	Misuse of the organisations 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	
HML73	Asset lifecycle security - Information and associated assets	Misuse of the organisations 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 security, compliance and resilience controls.	5	
HML74	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	
HML74	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 processed and/or stored.	5	
HML74	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	
HML75	Information security incident management - Learning from an information security incident	Organisations report all security incidents and near misses to the organisation's senior management or to the Board by a nominated Information Security Officer.	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	
HML75	Information security incident management - Learning from an information security incident	Organisations report all security incidents and near misses to the organisation's senior management or to the Board by a nominated Information Security Officer.	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 Security, Compliance & Resilience Program (SCRIP).	5	