Helper Document – HISF Guidance for suppliers

Health New Zealand
Te Whatu Ora

HISO 10029.4:2025 Last Updated: July 2026

National ID: 33462



Introduction

This document supports suppliers in the New Zealand health and disability sector to meet the requirements of the HISO 10029.4:2025 HISF Guidance for Suppliers. It aims to clarify the specific Secure Control Framework (SCF) that suppliers should adhere to, providing practical guidance and relevant resources to facilitate conformance to HISF. By utilizing this document, suppliers can more effectively implement and maintain robust security measures in alignment with industry best practices and Health New Zealand expectations.

The SCF is a meta-framework (framework of frameworks) that maps to more than 100 cybersecurity and privacy-related laws, regulations and industry. This Open-Source project has a library of more than 1200 controls and HISF requirements have been mapped to a sub-set of these controls. You can also download the SCF crosswalk matrix to assist in the development of a HISF-conforming cyber security programme.

This document covers key areas of HISF, such as Information Security Policy, Human Resource Security, Asset Lifecycle Security, Incident Management, Business Continuity, and more, all within the context of the HISF's Plan, Identify, Protect, Detect, and Respond framework. The content under the ‘HSUP Guidance’ column provides an outline of the additional level detailed guidance available in the HISO 10029.:2025 HISF Guidance for Suppliers.

To effectively use this document, suppliers should review each HISF requirement and its associated SCF controls to determine their organisation’s conformance to HISF. Links to publicly available resources, from New Zealand where possible or internationally where available, have also been provided. A self-audit of these HISF requirements will help to understand the specific actions needed to comply with each requirement. Suppliers can use this guide to assess their current security posture, identify gaps, and implement necessary improvements. It is recommended to integrate this guidance into existing security management processes and use it as a reference during audits and compliance checks.

Feedback on this document is highly encouraged to ensure its continued relevance and effectiveness. Users are invited to submit comments, suggestions, and any identified areas for improvement to CyberAssurance@TeWhatuOra.govt.nz. This feedback will be used to update and refine the document, ensuring it remains a valuable resource for suppliers in the health and disability sector working to protect sensitive health information.

Helper Document: HISF guidance for suppliers

Plan

- Information Security Policy
- Human Resource Security
- Asset Lifecycle Security
- Information Security Incident Management
- Business Continuity & Disaster Recovery Management
- Identity And Access Management
- Information Security Governance
- Physical And Environmental Security
- Cloud Security
- Systems Acquisition, Development & Maintenance
- Information Backups
- Change Management
- Patch And Vulnerability Management

Identify

- Human Resource Security
- Information Security Incident Management
- Business Continuity & Disaster Recovery Management
- Information Security Governance
- Compliance
- Cloud Security
- Systems Acquisition, Development & Maintenance
- Risk Management
- Change Management
- Supply Chain Management

Protect

- Asset Lifecycle Security
- Business Continuity & Disaster Recovery Management
- Cryptography
- Identity And Access Management
- Information Security Governance
- Physical And Environmental Security
- Remote Working
- Web Security
- Cloud Security
- Communications Security
- Information Backups
- Change Management
- Patch And Vulnerability Management
- Configuration Management
- Capacity Management
- Endpoint Security
- Data Leakage Prevention
- Supply Chain Management

Detect

- Business Continuity & Disaster Recovery Management
- Physical And Environmental Security
- Compliance
- Systems Acquisition, Development & Maintenance
- Information Backups
- Logging And Monitoring

Respond

- Human Resource Security
- Asset Lifecycle Security
- Information Security Incident Management

This page intentionally left blank.

Plan

Information Security Policy: HSUP01
The organisation has a clear information security policy, acceptable use policy, topic-specific policies and procedures to maintain information security.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	• Organisation's policies • Information security policy • Acceptable use policy • Topic-specific policies or procedures • Review of policies and procedures	NZISM 5.2: Information Security Policies
Rules of Behaviour	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behaviour for the use of technologies, including consequences for unacceptable behaviour.		
Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify, and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.		

Human Resource Security: HSUP02
Security roles and responsibilities of personnel are included within job descriptions.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	• Employment and contractual agreements • Roles and responsibilities	Planning and assigning responsibilities for protective security | Protective Security Requirements
Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.		

Human Resource Security: HSUP03
A breach of information by personnel is considered a security policy violation. Consequences of a security policy violation leads to a disciplinary process.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources

Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	Disciplinary process	Disciplinary process | Employment New Zealand
Workplace Investigations	HRS-07.1	Mechanisms exist to conduct employee misconduct investigations when there is reasonable assurance that a policy has been violated.		Office of the Privacy Commissioner | Privacy breaches

Human Resource Security: HSUP04

There are documented procedures for providing and revoking logical, and physical access when personnel join, have a role change or leave the organisation.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
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.	• Documented procedures • Onboarding and offboarding • The process for assigning or revoking physical and logical access • Access reviews	CISA and NSA:Identity and Access Management Recommended Best Practices for Administrators Identity and access management - NCSC.GOV.UK
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.		
Termination of Employment	IAC-07.2	Mechanisms exist to revoke user access rights in a timely manner, upon termination of employment or contract.		
Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.		
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).		
Role-Based Physical Access	PES-02.1	Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual.		

Asset Lifecycle Security: HSUP05 Asset management process(es) are in place.				
SCF Control	**SCF #**	**SCF Control Description**	**HSUP Guidance**	**Tools and Resources**
Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	• Asset Management process • Ownership of assets • Leased Devices	What is IT Asset Management (ITAM)? - ServiceNow

Asset Lifecycle Security: HSUP06 Processes are in place for media equipment management, decommissioning and secure disposal.				
SCF Control	**SCF #**	**SCF Control Description**	**HSUP Guidance**	**Tools and Resources**
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.	• Documented processes • Asset register • Removable storage media • Secure reuse or disposal	Office of the Privacy Commissioner | HIPC Factsheet 5 - Storage, Security, Retention and Disposal of Health Information Destroying information | Protective Security Requirements
Information Security Incident Management: HSUP07 An information security incident management process is in place.				
SCF Control	**SCF #**	**SCF Control Description**	**HSUP Guidance**	**Tools and Resources**

Incident Handling	IRO-02	Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery.	• Information security incident management • Reporting an information security incident • Testing of information security incident management process • Information security incident management plan	Cyber incidents – Health New Zealand | Te Whatu Ora
Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	• Communication during an information security incident • Resolution of an information security incident • Post-incident report	

Business Continuity and Disaster Recovery Management: HSUP08
Organisations have a documented, approved, business continuity and disaster recovery management, operational resilience policies and procedures in place.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	• Business continuity and disaster recovery plans (BCPs & DRPs) • Information security requirements	Continuity and contingency planning — business.govt.nz Managing business continuity | Protective Security Requirements

Identity And Access Management: HSUP09
Establish, document, approve, and implement rules to control physical and logical access to information and its assets.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources

Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	• Identity and access management policy or procedure	CISA and NSA:Identity and Access Management Recommended Best Practices for Administrators
Access To Information Systems	PES-03.4	Physical access control mechanisms exist to enforce physical access to critical information systems or sensitive/regulated data, in addition to the physical access controls for the facility.		

Information Security Governance: HSUP10
The organisation's Board or information security steering committee is accountable for information security governance.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	Information security governance	NCSC: Cyber Security Governance
Status Reporting to Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.		

Physical And Environmental Security: HSUP11
A documented policy and supporting procedures for maintaining physical security within the organisation is in place.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	• Physical and environmental security policy & procedures • Physical security risk assessments	CISA and NSA:Identity and Access Management Recommended Best Practices for Administrators
Site Security Plan (SitePlan)	PES-01.1	Mechanisms exist to document a Site Security Plan (SitePlan) for each server and communications room to summarize the implemented security controls to protect physical access to technology assets, as well as applicable risks and threats.		PSR: Physical Security

Physical And Environmental Security: HSUP12 A documented and approved procedure to remove papers and removable storage from easily accessible areas is to be implemented.				
SCF Control	**SCF #**	**SCF Control Description**	**HSUP Guidance**	**Tools and Resources**
Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	• Clear desk and clear screen procedures	CISA and NSA:Identity and Access Management Recommended Best Practices for Administrators
Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is stored.		
Removable Media Security	DCH-12	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.		
Cloud Security: HSUP13 Organisations have planned maintenance of information and services that are being provided to their customers via cloud services as per documented policies and agreements.				
SCF Control	**SCF #**	**SCF Control Description**	**HSUP Guidance**	**Tools and Resources**
Maintenance Operations	MNT-01	Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise.	• Cloud security policy • Cloud Service Agreement (CSA)	CSA Security Guidance for Cloud Computing | CSA
Systems Acquisition, Development and Maintenance HSUP14 Information systems are securely designed, and appropriate controls are implemented.				
SCF Control	**SCF #**	**SCF Control Description**	**HSUP Guidance**	**Tools and Resources**
System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	• Security engineering principles • Secure coding	Updated guidance: Principles and Approaches for Secure by

Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	• External tools and libraries • New acquisitions • Outsourced development	Design Software | National Cyber Security Centre DoD Enterprise DevSecOps Strategy Guide CIS Benchmarks
Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.		

Information Backups: HSUP15
A backup and recovery procedure is in place.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	• Backup and recovery procedure	Storing and backing up data - business.govt.nz
Information System Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of systems to a known state after a disruption, compromise or failure.		

Change Management: HSUP16
A documented process is in place for performing changes to new and existing systems or services.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources

Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	• Change management process • Change management document • Change management communication	Atlassian: What is IT change management? Definition, benefits and types
Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	• Unauthorised changes • Emergency or unplanned changes • Auditing changes	

Patch And Vulnerability Management
HSUP17
There is a documented and approved process for identifying vulnerabilities and updating patches on the organisation's systems, applications, tools, services, etc.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	• Patch management • Vulnerability management • Patch and vulnerability management process • Other procedures	NCSC vulnerability management - NCSC.GOV.UK
Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.		NIST: Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology
Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.		

Identify

Human Resource Security: HSUP18

Organisations, at a minimum, screen all personnel by verifying their identity, previous employment, applicable professional qualifications and criminal backgrounds before confirmation of employment.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	• Hiring process • Code of conduct • Supplier staff	PSR: Personnel Security

Human Resource Security: HSUP19

Organisations are to ensure:

- information security responsibilities are clearly defined and assigned
- a governance body or steering committee overseeing information security activities is in place
- there is at least one individual responsible for maintaining information security within the organisation.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	• Roles and responsibilities • Chief Information Security Officer (CISO) • Information Security Officer or Manager • Internal Auditor	• NCSC: Cyber Security Governance
Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.		
Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing data and technology-related risks.		

Human Resource Security: HSUP20

There has been an assessment of information security training needs, and a training plan is put in place.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	• Security awareness programme • Education and training • Leadership roles	Cyber security awareness – Health New Zealand | Te Whatu Ora

Information Security Incident Management: HSUP21

Organisations are to have roles and responsibilities determined to carry out the incident management process.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	• Roles and responsibilities	Cyber incidents – Health New Zealand | Te Whatu Ora

Business Continuity and Disaster Recovery Management: HSUP22

Establish criteria for developing business continuity, disaster recovery, operational resilience strategies, and capabilities based on disruption and impact to the organisation.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	• Business impact analysis (BIA)	Continuity and contingency planning — business.govt.nz Managing business continuity | Protective Security Requirements Storing and backing up data — business.govt.nz
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).		

Information Security Governance: HSUP23

Roles and responsibilities are defined and documented for planning, implementing, operating, assessing, and reporting on the organisation's information security requirements.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	• The Board (or steering committee) • Senior management (C-suite) • Chief Information Security Officer (CISO) • Security steering committee • Information Security Manager (ISM)	NCSC: Cyber Security Governance Planning and assigning responsibilities for protective security | Protective Security Requirements
Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing data and technology-related risks.		

Information Security Governance: HSUP24

Organisations are to integrate information security into project management.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	• Project management • Security risk assessment (SRA) • Security by design	Mind the gap: Governing cyber security risks - The Audit Office
Cybersecurity & Data Privacy in Project Management	PRM-04	Mechanisms exist to assess cybersecurity & data privacy controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.		

Compliance: HSUP25

Relevant legal, regulatory, and contractual requirements are identified and implemented.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	• Compliance	NCSC: Cyber Security Governance

Cloud Security: HSUP26

A risk assessment methodology and cloud assurance activities that support the use of cloud technologies are in place.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	• Risk assessment methodology • Risk assessment matrix • Performing security risk assessments (SRA) • Cloud assurance activities	NCSC: Cyber Security Governance Risks assessment for public cloud services | NZ Digital government

Systems Acquisition, Development and Maintenance: HSUP27

Business, customer, and security requirements are identified, documented, and approved when developing or acquiring applications.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical systems, applications and services to support the ongoing secure management of those assets.	• Business, customer and security requirements • Security requirements	What Is Requirements Management? | IBM
Cybersecurity & Data Privacy Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical systems, system components or services at pre-defined decision points in the Secure Development Life Cycle (SDLC).		Updated guidance: Principles and Approaches for Secure by Design Software | National Cyber Security Centre
Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity & data privacy that determines: • The resulting risk to organizational operations, assets, individuals and other organizations; and • Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.		

Risk Management: HSUP28

Risk assessments are performed on new, existing systems, and applications to understand the risks posed to the organisation while using them.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data.	• Security risk assessment (SRA) • Risk assessment methodology • Risk assessment matrix • Performing security risk assessments (SRA) • Risk register • Threat and vulnerability assessment (TVA) • Penetration testing • Control catalogue • Control validation plan (CVP) • Control validation audit (CVA)	NCSC: Cyber Security Governance Risks assessment for public cloud services | NZ Digital government

Change Management: HSUP29

The proposed changes are to be analysed for potential security threats and their impact on the organisation and their customers.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Security Impact Analysis for Changes	CHG-03	Mechanisms exist to analyse proposed changes for potential security impacts, prior to the implementation of the change.	• Change impact assessments • Penetration testing	Atlassian: What is IT change management? Definition, benefits and types

Supply Chain Management: HSUP67

Suppliers are to be systematically evaluated, and their information security activities are reviewed before and after onboarding of their systems and services.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	• Risk assessment activities • Use of additional security controls • Strong, collaborative security relationships • Continuous availability	Risks assessment for public cloud services | NZ Digital government
Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related services.		Supply chain security | National Cyber Security Centre
Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and audit External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity & data privacy controls.		

Protect

Asset Lifecycle Security: HSUP30

The organisation's information and associated assets are appropriately protected, used, and handled based on their importance.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	• Critical systems and services • Protection of devices • Physical security of devices	Office of the Privacy Commissioner | HIPC Factsheet 5 - Storage, Security, Retention and Disposal of Health Information What is IT Asset Management (ITAM)? - ServiceNow
Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.		
Endpoint Security	END-01	Mechanisms exist to facilitate the implementation of endpoint security controls.		

Business Continuity and Disaster Recovery Management: HSUP31

In the event of a disruption or failure, critical information or services are identified, and measures are taken for the continuity of services.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
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.	• Maintaining availability	Continuity and contingency planning — business.govt.nz Managing business continuity | Protective Security Requirements Storing and backing up data — business.govt.nz
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.		

Cryptography: HSUP32
Rules for effective use of cryptography, including encryption, and key management are defined and implemented.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	• Cryptography • Key management plan • Key lifecycle & authentication	SP 800-57 Part 1 Rev. 5: Recommendation for Key Management Part 1

Identity And Access Management: HSUP33
The complete lifecycle of the account(s) being used to access, process, or manage information and services is managed.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	• Unique identity • Access creation and modification	NZISM 16: System Access

Identity And Access Management: HSUP34
User accounts are authenticated and circumventing the authentication process is prevented.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
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).	• Authentication • Authentication mechanisms • Preventing authentication	Authentication - OWASP Cheat Sheet Series CISA and NSA:Identity and Access Management Recommended Best Practices for Administrators

Identity And Access Management: HSUP35

Access to information and its associated assets is defined and authorised according to the business, customer, and security requirements by adhering to the organisation's identity and access management policy or procedures.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	• Provision of access • Access reviews	Authorization - OWASP Cheat Sheet Series NZISM 16: System Access
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.		

Identity And Access Management: HSUP36

Organisations are to ensure that only authorised users, software components and services are provided with privileged access rights.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.	• Elevated or heightened permissions	Authorization - OWASP Cheat Sheet Series

Identity And Access Management: HSUP37

Access to source code, development tools, and software libraries are restricted, appropriately managed, and maintained.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	• Source code management	Authorization - OWASP Cheat Sheet Series
Access to Program Source Code	TDA-20	Mechanisms exist to limit privileges to change software resident within software libraries.		

Information Security Governance: HSUP38

Metrics affecting the organisation's cyber security posture are regularly reported to the Board, and any decisions made are clearly documented.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Status Reporting to Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.	• Measuring effectiveness of cyber security	InformationWeek:Measure Success: Key Cybersecurity Resilience Metrics
Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.		

Physical And Environmental Security: HSUP39

Update, protect and maintain the devices installed as physical security safeguards including the utilities.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	• External and environmental threats • Site plan • Maintenance of utilities • Security of cabling	PSR: Physical Security

Physical And Environmental Security: HSUP40

Secure areas of the organisation are protected from unauthorised personnel.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
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).	• Visitor management • Visitor management system • Temporary access cards • Secure or restricted areas	Specific security measures | Protective Security Requirements
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.		

Remote Working: HSUP41

Secure mechanisms are available and supported by a documented policy or guidelines to connect to the organisations or customer's network.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Identification & Authentication for Third Party Systems & Services	IAC-05	Mechanisms exist to identify and authenticate third-party systems and services.	• Remote working • Remote working procedures • Remote working guidelines	Working Remotely: Getting Started on Cloud Security | National Cyber Security Centre
Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).		

Web Security: HSUP42

Security controls are implemented if the organisation is developing the web applications to protect them and their customers from potential cyber-attacks.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
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.	• Web applications • Web security	OWASP Top Ten | OWASP Foundation
Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to update products, including systems, software and services, to improve functionality and correct security deficiencies.		
Secure Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.		

Cloud Security: HSUP43
The organisation's architectural strategy supports the adoption of cloud technologies.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
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.	• Cloud computing • Cloud computing services • Cloud computing deployments • Cloud adoption strategy • Cloud security risk assessments • Content delivery network (CDN)	Risks assessment for public cloud services | NZ Digital government

Cloud Security: HSUP44
Organisations are to make use of developed and configured APIs for secure transfer of information between different cloud components.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Application & Program Interface (API) Security	CLD-04	Mechanisms exist to ensure support for secure interoperability between components with Application & Program Interfaces (APIs).	• Cloud API Security • Best practices	API guidelines — Part B: API security 2022 | NZ Digital government Knowledge hub – Health New Zealand | Te Whatu Ora

Cloud Security: HSUP45
Organisations are to ensure that appropriate controls are implemented to protect information in a multi-tenant cloud environment.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
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.	• Multi-tenant environment • Shared responsibility model	Risks assessment for public cloud services | NZ Digital government

Communications Security: HSUP46

Networks and network devices that are used within the organisation are to be securely managed.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	• Network security • Zero trust architecture • Virtual networks	What is IT Asset Management (ITAM)? - ServiceNow CIS Benchmarks
System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.		
Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).		

Communications Security: HSUP47

The systems and applications that are used to process, store, or transmit information are connected to a separate, dedicated network.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Isolation of Information System Components	NET-03.7	Mechanisms exist to employ boundary protections to isolate systems, services and processes that support critical missions and/or business functions.	• Network segmentation and segregation • Virtual local area network (VLAN) • Access to networks	Segregate Dev, Testing, and Production Environments | CSA
Network Segmentation (macro-segmentation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.		

Information Backups: HSUP48

Backup copies of information, software, services provided, and relevant systems are protected and maintained in accordance with the backup and recovery procedures.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	• Backups and recovery • Backup and recovery plans • Backup storage • Backup retention	Storing and backing up data - business.govt.nz
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.		

Information Backups: HSUP49

Backups are tested for their restoration in accordance with the documented backup and recovery procedures. Organisations are able to access restored backups as well.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
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.	• Backup restoration	Storing and backing up data - business.govt.nz

Change Management: HSUP50

Organisations developing inhouse systems, applications, or services are to maintain separate production and non-production environments.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Separation of Development, Testing and Operational Environments	TDA-08	Mechanisms exist to manage separate development, testing and operational environments to reduce the risks of unauthorized access or changes to the operational environment and to ensure no impact to production systems.	• Separate environments • Development environment • Test environment • Staging environment • Production environment	Segregate Dev, Testing, and Production Environments | CSA

Patch And Vulnerability Management: HSUP51

Identified vulnerabilities or unpatched systems, services or applications are properly identified, tracked, and remediated.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	• Unpatched software or known vulnerabilities • Logging and monitoring • Cloud services	NCSC vulnerability management - NCSC.GOV.UK
Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.		

Configuration Management: HSUP52

Organisations have a standardised baseline configuration in place for new and existing systems, services, and applications.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	• Configuration management • Baseline configurations • System hardening • Open-source software	CIS Benchmarks

Capacity Management: HSUP53

The capacity requirements for maintenance of information processing facilities, communication, and environmental support during contingency operations are met.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	• Capacity management	Continuity and contingency planning — business.govt.nz Managing business continuity | Protective Security Requirements Storing and backing up data — business.govt.nz
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.		

Endpoint Security: HSUP54

Information, services, and applications on organisation systems and associated assets are protected against malware.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	• Malware • Protection against malware	Ensure Your OS Antivirus and Anti-Malware Protections are Active | CISA

Data Leakage Prevention: HSUP55

Organisations are to detect and prevent data leakage through the unauthorised disclosure and siphoning of information by individuals, systems, or services.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Monitoring For Information Disclosure	MON-11	Mechanisms exist to monitor for evidence of unauthorized exfiltration or disclosure of non-public information.	• Data leakage prevention • Tools and technologies • Implementing DLP	Reducing data exfiltration by malicious insiders - NCSC.GOV.UK
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.		

Supply Chain Management: HSUP68

The organisation's information security requirements are to be included in the agreements with the suppliers.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Third-Party Contracts	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third parties, reflecting the organization's needs to protect its systems, processes and data.	• Agreements with suppliers • Reporting metrics	Security governance (GOV) | Protective Security Requirements

Detect

Business Continuity and Disaster Recovery Management: HSUP56
The lessons learned from business continuity and disaster recovery testing are reflected in the established and implemented information security controls.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
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.	• ICT readiness	AWQ: Root Cause Analysis Continuity and contingency planning — business.govt.nz

Physical And Environmental Security: HSUP57
Installed physical and environmental security mechanisms are monitored for potential security incidents.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	• Continuous monitoring	PSR: Physical Security

Compliance: HSUP58
Regular reviews are performed to confirm that the legal, regulatory, statutory, and contractual requirements are met.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's executive leadership.	• Compliance reviews • Review of policies, procedures and other relevant documents • Planning an audit • Components of an audit • Self-assessment	NCSC: Cyber Security Governance ISACA:2017 Volume 4 IS Audit Basics Audit Programs ISACA:2023 Volume 6 The Risk and Control Self Assessment
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.		
Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.		

Systems Acquisition, Development and Maintenance: HSUP59
Independent security reviews are defined and implemented before any new or major upgrades on systems are moved to the production environment.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy assessment and authorization controls.	• Independent security review • Security testing • Outsourced services	Understanding the information security lifecycle | Protective Security Requirements
Assessments	IAO-02	Mechanisms exist to formally assess the cybersecurity & data privacy controls in systems, applications and services through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.		Trust Framework for Digital Identity templates and guidance - dia.govt.nz

Information Backups: HSUP60
Authorised personnel or teams are alerted upon unsuccessful backups.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	• Monitoring	Storing and backing up data - business.govt.nz
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.		
Automated Alerts	MON-01.12	Mechanisms exist to automatically alert incident response personnel to inappropriate or anomalous activities that have potential security incident implications.		
System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data privacy and supply chain activities to achieve integrated situational awareness.		

Logging And Monitoring: HSUP61

The activities performed on the information processing systems, services, and applications are logged and stored as per the organisation's (and the customer's) logging and auditing requirements.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	• Logging and auditing • Logging and auditing requirements • Recording an event • Log analysis • Collection and storage of logs • Real-time monitoring	Best practices for event logging and threat detection | Cyber.gov.au
Content of Event Logs	MON-03	Mechanisms exist to configure systems to produce event logs that contain sufficient information to, at a minimum: •Establish what type of event occurred; •When (date and time) the event occurred; •Where the event occurred; •The source of the event; •The outcome (success or failure) of the event; and •The identity of any user/subject associated with the event.		
Audit Trails	MON-03.2	Mechanisms exist to link system access to individual users or service accounts.		

Logging And Monitoring: HSUP62

The information processing systems, applications, devices, and services are synchronised to an approved time source.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Synchronization With Authoritative Time Source	MON-07.1	Mechanisms exist to synchronize internal system clocks with an authoritative time source.	• Medical Device Relevance	Best practices for event logging and threat detection | Cyber.gov.au

Respond

Human Resource Security: HSUP63

Breach of employment and supplier agreements are enforced.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	• Agreement breach governance	Disciplinary process | Employment New Zealand
Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third parties, reflecting the organization's needs to protect its systems, processes and data.		Security governance (GOV) | Protective Security Requirements

Asset Lifecycle Security: HSUP64

Misuse of the organisation's assets is investigated, and documented procedures are followed as stated in the acceptable use policy, contractor agreements, or service agreements.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	• Information security requirements • Documented procedures	Disciplinary process | Employment New Zealand
Workplace Investigations	HRS-07.1	Mechanisms exist to conduct employee misconduct investigations when there is reasonable assurance that a policy has been violated.		Security governance (GOV) | Protective Security Requirements
Monitoring for Third-Party Information Disclosure	TPM-07	Mechanisms exist to monitor for evidence of unauthorized exfiltration or disclosure of organizational information.		
Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and audit External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity & data privacy controls.		

Information Security Incident Management: HSUP65

Organisations report all security incidents and near misses to their senior management or to the Board by a nominated Information Security Officer.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Status Reporting to Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.	• Lessons learned from information security incidents	NCSC: Cyber Security Governance Security governance (GOV) | Protective Security Requirements Report an incident | CERT NZ
Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: • Internal stakeholders; • Affected clients & third parties; and • Regulatory authorities.		

Information Security Incident Management: HSUP66

Evidence gathered as part of the incident management process is appropriately protected.

SCF Control	SCF #	SCF Control Description	HSUP Guidance	Tools and Resources
Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	• Collection and protection of evidence	Reporting incidents and conducting security investigations | Protective Security Requirements
Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is stored.		
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.		

Index of links in tools and resources

Link	Controls	HISF Requirement Statement
AWQ: Root Cause Analysis	BCD-05	HSUP56
API guidelines — Part B: API security 2022 | NZ Digital government	CLD-04	HSUP44
Atlassian: What is IT change management? Definition, benefits and types	CHG-01, CHG-02, CHG-03	HSUP29, HSUP16
Authentication - OWASP Cheat Sheet Series	IAC-01.2	HSUP34
Authorization - OWASP Cheat Sheet Series	IAC-15, IAC-07, IAC-08, IAC-16	HSUP35, HSUP36, HSUP37,
Best practices for event logging and threat detection	MON-03.2, MON-03, MON-01, MON-07.1	HSUP61, HSUP62
NZISM 16: System Access	IAC-15	HSUP33, HSUP35
CIS Benchmarks	AST-01, NET-01, SEA-01, CFG-02, GOV-15	HSUP46, HSUP52, HSUP14
CISA and NSA:Identity and Access Management Recommended Best Practices for Administrators	DCH-01, PES-01, DCH-12, DCH-01.2, PES-01.1 IAC-07.1, PES-02, IAC-08, PES-02.1, IAC-07.2, IAC-07, IAC-01.2, IAC-20, PES-03.4	HSUP04, HSUP09, HSUP11, HSUP12, HSUP34
SP 800-57 Part 1 Rev. 5: Recommendation for Key Management Part 1	CRY-01	HSUP32

Link	Controls	HISF Requirement Statement
Continuity and contingency planning — business.govt.nz	BCD-01, CAP-01, BCD-05, BCD-02.2, BCD-01.4, BCD-02.1	HSUP08, HSUP22, HSUP31, HSUP56, HSUP58
CSA Security Guidance for Cloud Computing | CSA	MNT-01	HSUP13
Cyber incidents – Health New Zealand | Te Whatu Ora	IRO-02, IRO-04, HRS-03	HSUP21, HSUP07
Cyber security awareness – Health New Zealand | Te Whatu Ora	HSUP07	HSUP20
Destroying information | Protective Security Requirements	AST-09	
Disciplinary process | Employment New Zealand	HRS-07, HRS-07.1	HSUP63, HSUP64, HSUP03
DoD Enterprise DevSecOps Strategy Guide	GOV-15, SEA-01, CFG-02	HSUP14
Ensure Your OS Antivirus and Anti-Malware Protections are Active | CISA	END-04	HSUP54
Identity and access management - NCSC.GOV.UK	IAC-07, IAC-07.1, IAC-07.2, IAC-08, PES-02, PES-02.1	HSUP04
Identity and Access Management Recommended Best Practices for Administrators	IAC-07.1, PES-02, IAC-08, PES-02.1, IAC-07.2, IAC-07, IAC-01.2, IAC-20, PES-03.4	HSUP04, HSUP09, HSUP11, HSUP12, HSUP34
InformationWeek:Measure Success: Key Cybersecurity Resilience Metrics	GOV-05, GOV-01.2	HSUP38

Link	Controls	HISF Requirement Statement

ISACA:2017 Volume 4 IS Audit Basics Audit Programs	CPL-02, GOV-03, CPL-02.1	HSUP58
ISACA:2023 Volume 6 The Risk and Control Self Assessment	CPL-02, GOV-03, CPL-02.1	HSUP58
Atlassian: What is IT change management? Definition, benefits and types	CHG-01, CHG-02, CHG-03	HSUP29, HSUP16
Knowledge hub – Health New Zealand | Te Whatu Ora	CLD-04	HSUP44
Trust Framework for Digital Identity templates and guidance - dia.govt.nz	IAO-02, IAO-01	HSUP59
Supply chain security | National Cyber Security Centre	TPM-01, TPM-08	HSUP67, HSUP68
Security governance (GOV) | Protective Security Requirements	TPM-05, TPM-07, TPM-08, IRO-10	HSUP63, HSUP64, HSUP65, HSUP68
Managing business continuity | Protective Security Requirements	BCD-01, CAP-01, BCD-02.2, BCD-01.4, BCD-02.1	HSUP08, HSUP22, HSUP31, HSUP53
NCSC vulnerability management - NCSC.GOV.UK	VPM-05, VPM-01, VPM-02, VPM-06	HSUP51, HSUP17
NZISM 5.2: Information Security Policies	GOV-02, HRS-05.1, OPS-01.1	HSUP01
Mind the gap: Governing cyber security risks - The Audit Office	PRM-04, GOV-15	HSUP24
NCSC: Cyber Security Governance	GOV-04, CPL-02, IRO-10, RSK-04, RSK-01, GOV-03, GOV-01.2, CPL-01, GOV-01.1, CPL-02.1, GOV-04.1	HSUP58, HSUP65, HSUP19, HSUP23, HSUP25, HSUP28, HSUP10
NIST: Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology	VPM-01, VPM-02, VPM-05	HSUP17

PSR: Personnel Security	HRS-04	HSUP18

Link	Controls	HISF Requirement Statement
Office of the Privacy Commissioner | HIPC Factsheet 5 - Storage, Security, Retention and Disposal of Health Information	DCH-02 DCH-01 END-01 AST-09	HSUP30, HSUP06
Office of the Privacy Commissioner | Privacy breaches	HRS-07, HRS-07.1	HSUP03
OWASP Top Ten | OWASP Foundation	TDA-01.1, TDA-06, TDA-01	HSUP42
Planning and assigning responsibilities for protective security | Protective Security Requirements	GOV-04, HRS-01, HRS-03	HSUP59, HSUP53, HSUP39, HSUP39, HSUP22, HSUP31, HSUP06, HSUP08, HSUP02
PSR: Physical Security	PES-01	HSUP39
Reducing data exfiltration by malicious insiders - NCSC.GOV.UK	NET-17, MON-11	HSUP55
Report an incident | CERT NZ	IRO-10, GOV-01.2	HSUP66
Reporting incidents and conducting security investigations | Protective Security Requirements	IRO-08, DCH-01, DCH-01.2	HSUP66
Risks assessment for public cloud services | NZ Digital government	CLD-02, CLD-06, RSK-04, RSK-01, TPM-04.1	HSUP43, HSUP45, HSUP26, HSUP28, HSUP67
Segregate Dev, Testing, and Production Environments | CSA	NET-03.7, NET-06, TDA-08	HSUP32
Specific security measures | Protective Security Requirements	PES-03, PES-04	HSUP40

Link	Controls	HISF Requirement Statement
Storing and backing up data - business.govt.nz	MON-01.12, MON-01.4, BCD-11.10, BCD-01, CAP-01, BCD-11, BCD-12, BCD-11.1, BCD-02.2, BCD-01.4, BCD-02.1	HSUP56, HSUP48, HSUP49, HSUP53, HSUP22, HSUP31, HSUP15, HSUP08, HSUP60, HSUP65
Understanding the information security lifecycle | Protective Security Requirements	IAO-02, IAO-01	HSUP59
Updated guidance: Principles and Approaches for Secure by Design Software | National Cyber Security Centre	PRM-06, GOV-15, PRM-05, SEA-01, CFG-02, PRM-05, AST-01.2	HSUP27, HSUP14
What is IT Asset Management (ITAM)? - ServiceNow	AST-01, DCH-02, DCH-01, END-01, NET-01, CFG-02	HSUP46, HSUP30, HSUP05
What Is Requirements Management? | IBM	PRM-05, AST-01.2	HSUP27
Working Remotely: Getting Started on Cloud Security | National Cyber Security Centre	IAC-05, NET-01	HSUP41



Health New Zealand
Te Whatu Ora

Te Kāwanatanga o Aotearoa
New Zealand Government