

Health Information Security Framework

HISO 10029:2022

Released December 2022

Citation: Te Whatu Ora – Health New Zealand. 2022. *HISO 10029:2022 Health Information Security Framework*. Wellington: Te Whatu Ora – Health New Zealand.

Published in December 2022 by Te Whatu Ora – Health New Zealand
PO Box 793, Wellington 6140, New Zealand

ISBN 978-1-99-106707-4 (online)

Te Whatu Ora
Health New Zealand

This document is available at [tewhatauora.govt.nz](https://www.tewhatauora.govt.nz)



This work is licensed under the Creative Commons Attribution 4.0 International licence. In essence, you are free to: share ie, copy and redistribute the material in any medium or format; adapt ie, remix, transform and build upon the material. You must give appropriate credit, provide a link to the licence and indicate if changes were made.

Contents

1	Purpose	4
2	Scope	5
3	Background	6
4	Commitment to Māori co-design	7
5	Framework essentials	9
5.1	HISF Obligations	11
5.2	HISF Functional Processes	12
5.3	Segmentation model	13
5.4	Controls	15
5.5	Cyber security requirements	16
5.6	Guidance	18
5.7	Tools and templates	18
6	References	19
	Appendix A – Glossary	21

List of Figures

Figure 1:	HISF Strategy Map	9
Figure 2:	Expected Outcomes	10
Figure 3:	HISF Foundational Building Blocks	10
Figure 4:	HISF Functional Processes	12
Figure 5:	Segmentation with risk characteristics	13
Figure 6:	HISF Maturity Assessment Scale	15
Figure 7:	Refreshed HISF Framework	16
Figure 8:	Five HISF functional processes with sub-categories	17

1 Purpose

The Health Information Security Framework (framework) is a set of materials published to guide the New Zealand health sector in the secure use and management of health information and information technology.

The HISO 10029:2023 Health Information Security Framework is the latest edition, designed for the reshaped operating environment introduced by the 2022 health reforms. The framework provides a way to approach cyber security that can be easily understood and adopted across the broad spectrum of health organisations and their industry partners.

The framework supports health system investments that will:

- improve system resilience by addressing issues resulting from technology infrastructure and systems that are out-of-support and no longer fit for purpose
- improve data and analytics capability across the health system so that equity issues can be targeted more effectively and to drive the development of new models of care
- improve information sharing between providers to facilitate greater collaboration and coordination of care
- empower New Zealanders to better manage their own health and wellbeing by providing more digital options for accessing care and information.

2 Scope

This framework covers the security of all health information that is collected and used within New Zealand; and wherever it is stored. All personal health information is treated as MEDICAL IN CONFIDENCE¹ and given an equal level of protection unless otherwise classified.

The framework comprises this umbrella document and a set of companion documents that are being developed to provide targeted guidance for different types of organisations and different risk profiles.

The framework incorporates a strategy map, set of obligations and guiding principles, with controls mapping to leading industry security frameworks, including the New Zealand Information Security Manual (NZISM), Protective Security Requirements (PSR), Center for Internet Security (CIS), Cloud Security Alliance (CSA) and CERT NZ Critical Controls.

Privacy is covered by the **Health Information Privacy Code 2020** and is not within the scope of this framework.

The forthcoming parts of the framework are:

- HISO 10029.1:2023 Health Information Security Framework Guidance for Hospitals
- HISO 10029.2:2023 Health Information Security Framework Guidance for Micro to Small Organisations
- HISO 10029.3:2023 Health Information Security Framework Guidance for Medium to Large Organisations
- HISO 10029.4:2023 Health Information Security Framework Guidance for Suppliers

¹ The New Zealand government defines 'IN CONFIDENCE' as information that if released "would be likely to prejudice the maintenance of law and order, impede the effective conduct of government in New Zealand or affect adversely the privacy of its citizens". Department of Prime Minister and Cabinet, Cabinet Office Circular CO (08) 01 <http://www.dpmc.govt.nz/cabinet/circulars/co08/1>

From a practitioner viewpoint, IN CONFIDENCE mirrors doctor patient confidentiality and means that a person's health information won't be disclosed unless consented to or authorised by that person (eg, through a privacy fact sheet), by another authorised person, under statutory authority or by a legal instrument (eg, an Approved Information Sharing Agreement).

3 Background

The first edition of the Health Information Security Framework published in 2009 covered security essentials and included a set of security policies and procedures. A technical specifications register was added in 2013. In 2015, a fully revised second edition was published to bring the framework up-to-date with the International Organisation for Standardization (ISO).

In a rapidly changing security environment, the 2015 edition became no longer fit for purpose, having proven challenging for health providers and their industry partners to understand, adopt and use – particularly smaller organisations with limited access to information security expertise. The ever-changing information security landscape, including the increasing adoption of cloud-based solutions, meant that new and heightened cyber security risks needed to be addressed. The 2015 edition also did not directly cater for Hauora Māori.

The new framework presented here switches its focus from the ISO-centric model used previously to the development of a National Institute of Standards and Technology (NIST) Cybersecurity Framework-based model for Aotearoa. This provides a better fit, more aligned to national and international best practice, without losing sight of ISO standards. NIST is the National Institute of Standards and Technology in the United States.

4 Commitment to Māori co-design

There is commitment to Māori co-design in producing, maintaining and driving adoption of the framework. This commitment is part of ensuring we meet our obligations under the Ministry of Health's Te Tiriti o Waitangi Framework.

Expression of Te Tiriti

The text of Te Tiriti, including the preamble and the three articles, along with the Ritenga Māori declaration, are the enduring foundation of our approach. Based on these foundations, we will strive to achieve the following four goals, each expressed in terms of mana.

- **Mana whakahaere:**
The effective and appropriate stewardship or kaitiakitanga over the health and disability system. This goes beyond the management of assets or resources.
- **Mana motuhake:**
Enabling the right for Māori to be Māori (Māori self-determination); to exercise their authority over their lives, and to live on Māori terms and according to Māori philosophies, values and practices including tikanga Māori.
- **Mana tangata:**
Achieving equity in health and disability outcomes for Māori across the life course and contributing to Māori wellness.
- **Mana Māori:**
Enabling Ritenga Māori (Māori customary rituals) which are framed by te ao Māori (the Māori world), enacted through tikanga Māori (Māori philosophy and customary practices) and encapsulated within mātauranga Māori (Māori knowledge).

Approach to achieving these goals

The principles of Te Tiriti o Waitangi, as articulated by the Courts and the Waitangi Tribunal, provide the framework for how we will meet our obligations under Te Tiriti in our day-to-day work.

- **Tino rangatiratanga:**
The guarantee of tino rangatiratanga, which provides for Māori self-determination and mana motuhake in the design, delivery, and monitoring of health and disability services.

- **Equity:**
The principle of equity, which requires the Crown to commit to achieving equitable health outcomes for Māori.
- **Active protection:**
The principle of active protection, which requires the Crown to act, to the fullest extent practicable, to achieve equitable health outcomes for Māori. This includes ensuring that it, its agents, and its Treaty partner are well informed on the extent, and nature, of both Māori health outcomes and efforts to achieve Māori health equity.
- **Options:**
The principle of options, which requires the Crown to provide for and properly resource kaupapa Māori health and disability services. Furthermore, the Crown is obliged to ensure that all health and disability services are provided in a culturally appropriate way that recognises and supports the expression of hauora Māori models of care.
- **Partnership:**
The principle of partnership, which requires the Crown and Māori to work in partnership in the governance, design, delivery, and monitoring of health and disability services. Māori must be co-designers, with the Crown, of the health system for Māori.

5 Framework essentials

The framework is an approach to cyber security rather than a ‘yes’ and ‘no’ standard. It is more about how we think as we implement Te Pae Tata Interim New Zealand Health Plan 2022 and Te Whatu Ora’s operating model.

The framework is designed to motivate, build capability and remove barriers for health care providers.

Strategy map

Our strategy map details the sector and user outcomes that the framework supports, the behaviour change levers the framework will employ, the foundational building blocks of the framework, and the implementation support activities required to sustain it. The strategy was developed through a co-design process with representatives from organisations across the health and disability sector. The strategy is one pillar of Te Whatu Ora’s three-year Cyber Security Uplift Programme (2022-2024). The programme is designed to uplift cyber security within three workstreams: Leadership Capability and Assurance, Sector Protect and Sector Detect, Respond Recover.

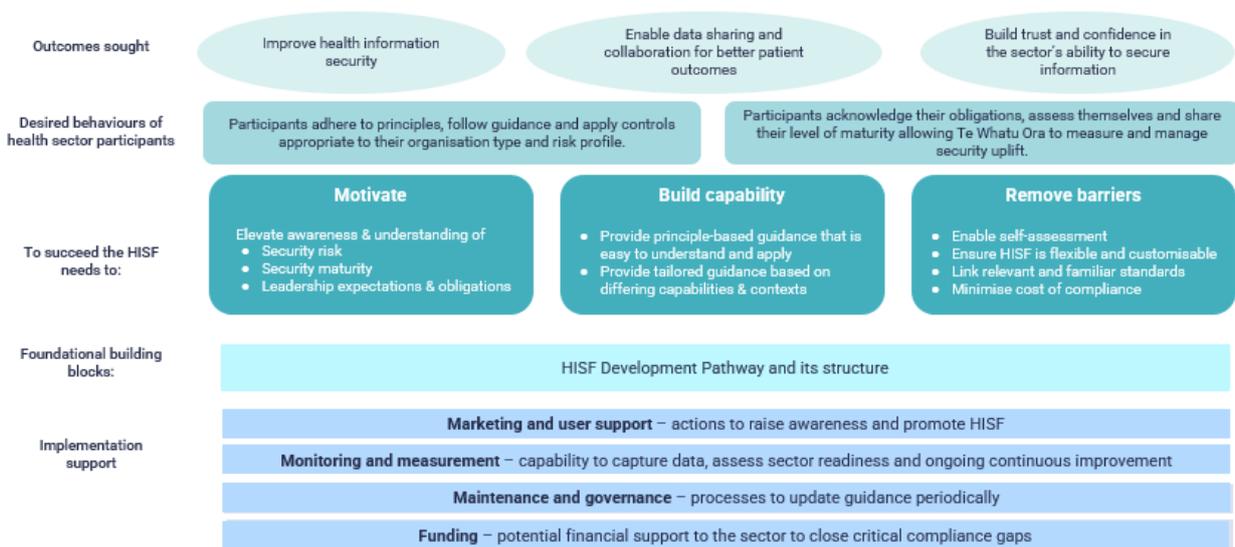


Figure 1: Strategy map

Our strategy map supports the following outcomes:

Outcomes sought	This could be observed by
<ul style="list-style-type: none"> • Improve health information security • Enable sharing of personal health information to collaborate with organisations • Build trust and confidence in the health sector's ability to secure information 	<ul style="list-style-type: none"> • Better incident response and more visible reporting • Improved patient wellbeing and clinical outcomes • Improved engagement and wide adoptions of the framework

Figure 2: Expected outcomes

Successful implementation of this framework will require the participants to:

- use the framework as a key mechanism for assessing and improving information security maturity, and manage the organisation's risk profile
- acknowledge their obligations, assess themselves and share their level of maturity, allowing Te Whatu Ora and other key stakeholders to measure and manage security uplift.

The framework has the following seven foundational building blocks:

Building Block	Description
Obligations	To uphold and maintain adherence to the wairua or spirit and intent of the information security principles, in all endeavours to achieve and maintain health information security.
Functional Processes	Provide strategic guidance on how an organisation can protect their systems and data from cyber threats.
Segmentation Model	Health sector segments so that the framework is tailored appropriately to different types of organisations and audiences.
Controls	Safeguards or countermeasures prescribed for an information system or an organisation, designed to protect the confidentiality, integrity, and availability of the system and its information.
Requirements	Plain language descriptions of what information security practices are required and are the core of the framework for maturity assessment.
Guidance	The activities the organisation needs to implement to meet the requirement.
Tools and Templates	Segment-specific toolkits and templates will be available for reference.

Figure 3: Foundational building blocks

The four implementation support elements underpin these foundational building blocks. Namely, marketing and user support, monitoring and measurement, maintenance and governance, and funding.

5.1 Obligations

All organisations that collect, process or store personal health information (PHI) and patient personally identifiable information (PII) related to New Zealanders have the following obligations under our framework:

- **Te Tiriti o Waitangi**
ensure the application of the framework progresses the health and well-being of Māori, does not place undue burden on the Māori health sector and that Māori data is collected, stored, and transferred in ways that enable and reinforces the capacity of Māori to exercise kaitiakitanga over Māori data.
- **Confidentiality**
ensure personal health information is accessible to those authorised for access.
- **Integrity**
ensure the safeguarding, the accuracy and completeness of information, its handling and processing.
- **Availability**
ensure authorised users have access to personal health information when required.

5.2 Functional processes

Our framework defines five functional processes (Plan, Identify, Protect, Detect, and Respond) that support the four obligations as described in the previous section.

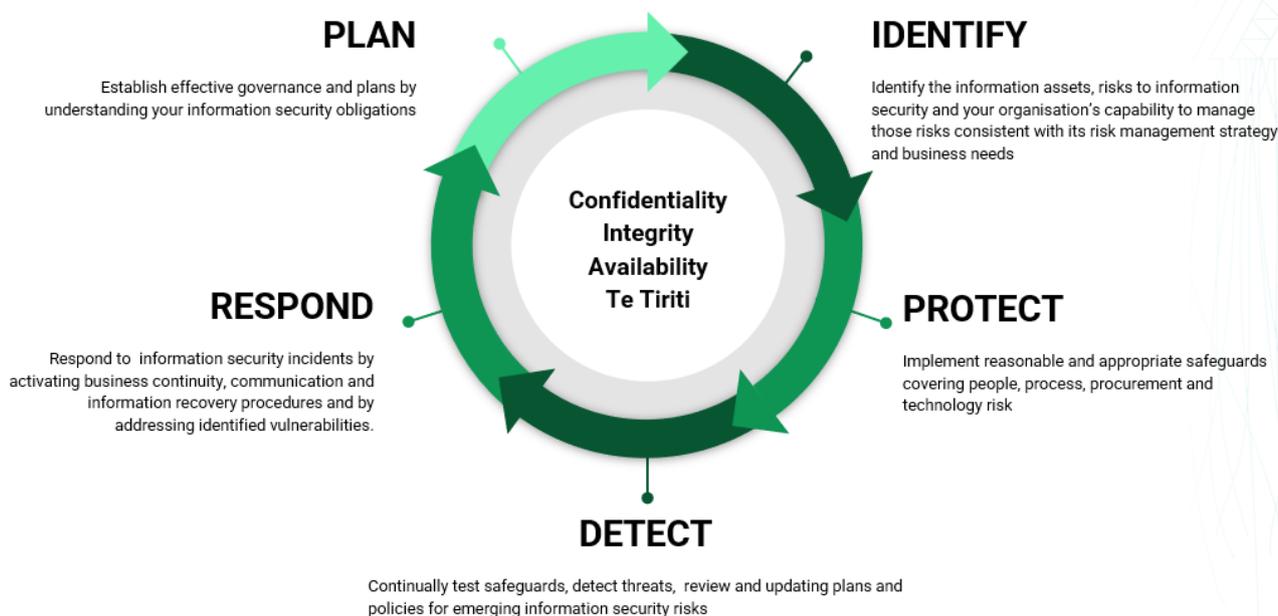


Figure 4: HISF Functional Processes

The five functional processes are a high-level grouping of the elements that represent the primary pillars for a successful and holistic cyber security framework, adapted from the NIST Cybersecurity Framework².

Overall, the functional processes are designed to reinforce the continuous nature of organisational behaviour and practice with respect to information security as well as:

- describe required organisational capabilities to manage information security
- be understandable to everyone
- be applicable to any size or type of organisation and their information security risk profile
- span both prevention and response to vulnerabilities and threats.

² <https://www.nist.gov/cyberframework>

5.3 Segmentation model

The segmentation model conceptualises types of health sector organisations that share similar information security risk profiles and thus similar requirements for managing information security risk.

The purpose of the segmentation model is to make it easier for health care providers to recognise the nature of information security risk they face and to easily find the guidance and controls most appropriate to them.

The model recognises diversity and the broad spectrum of organisations that comprise the New Zealand health and disability sector with varying risk profiles (ie, likelihood of risks and potential impacts/ consequences).

5.3.1 Common risk characteristics

Based on the co-design approach, the risk characteristics below are identified as common across each segment. Controls are designed based on the implementation capabilities and areas of expertise across each segment.

		Hospitals (Public and private)	Micro to small organisations	Medium to large organisations	Suppliers (e.g., Non-clinical, IT)
	Risk Characteristics				
Risk	Information asset value/sensitivity	↓	↓	↓	↓
	Information volume				
	Size of surface area				
	Information security architecture risk	↓	↓	↓	↓

Figure 5: Segmentation with risk characteristics

The key health segments are grouped vertically. Definitions of the horizontal grouping of risk characteristics are as follows:

- Information asset value/sensitivity**
 is the nature of the personal health information captured, processed, stored, or transmitted by an organisation and how valuable it may be considered by the individuals who provide it to an organisation.
- Information volume**
 is the absolute quantity of personal health information captured, processed, stored, or

transmitted by an organisation. This would include the total number of individual records held and the number of health information data points for each individual.

- **Size of surface area**
this relates to the number of endpoints (e.g., devices, APIs, servers, systems, and platforms) that an organisation is responsible for managing and therefore securing.
- **Information security architecture risk**
this relates to the nature of the information systems that an organisation is responsible for securing (e.g., on-premises infrastructure, cloud-based platforms and software as a service and use of third-party vendors for services and security).

5.3.2 Segmentation and maturity

The maturity of the practices and behaviours of health and disability organisations in regard to the functional processes described by the HISF varies both between segments and within segments.

We recognise varying levels of maturity across the health sector in two ways:

- Providing different guidance and requirements for organisations in each segment. Some segments will have a comprehensive implementation guide, while others will have a simplified guide based on the nature of the audience. The guidance will contain ideal practices that are articulated by the combination of requirements and controls defined under each of the five functional processes for organisations in a specific segment.
- Providing a maturity assessment model to allow organisations to assess maturity against the guidance and requirements for organisations in each segment.

Our maturity assessment model uses a rating scale to assess the extent to which requirements or security controls are implemented. A self-assessment at an organisational level against each requirement per segment will be included with the framework in future. The maturity assessment below contains a scale of 1 to 5.

Maturity Assessment Scale				
1-None	2-Emerging	3-Partially Applied	4-Maturing	5-Embedded
No understanding of this cyber security concept and/or no control is in place to support the requirement.	Not formally in place but some form of controls exists to support the requirement. These are not documented, and/or there are significant gaps in their application to areas or systems.	Controls exist and are applied, but they are not thoroughly formalised or documented, and/or they are not consistently applied to all functional areas or systems.	Controls exist and are formally documented. They are regularly applied across most functional areas and systems. There is some monitoring of control effectiveness and attempts at control improvement.	Robust controls are in place with documentation. They cover all functional areas and systems and are periodically reviewed for monitoring and continuous improvement. The requirement is completely met.

Figure 6: Maturity Assessment Scale

5.4 Controls

Controls are safeguards or countermeasures to detect, avoid, mitigate, or reduce organisational, people, physical and technology risks.

Mappings to control catalogues

Our framework does not create a duplicate of relevant ISO standards. Rather it maps to the relevant and dominant control catalogues such as NZISM, Center for Internet Security (CIS), Cloud Controls Matrix (CSA), ISO 27002, ISO 27799, HIPAA, PSR and CERT NZ Top Ten.

The framework is a medium through which the guidance to organisations about relevant controls for each is tailored based on their risk segment and maturity levels.

Mappings between the relevant controls, the requirements to various control catalogues are as follows:

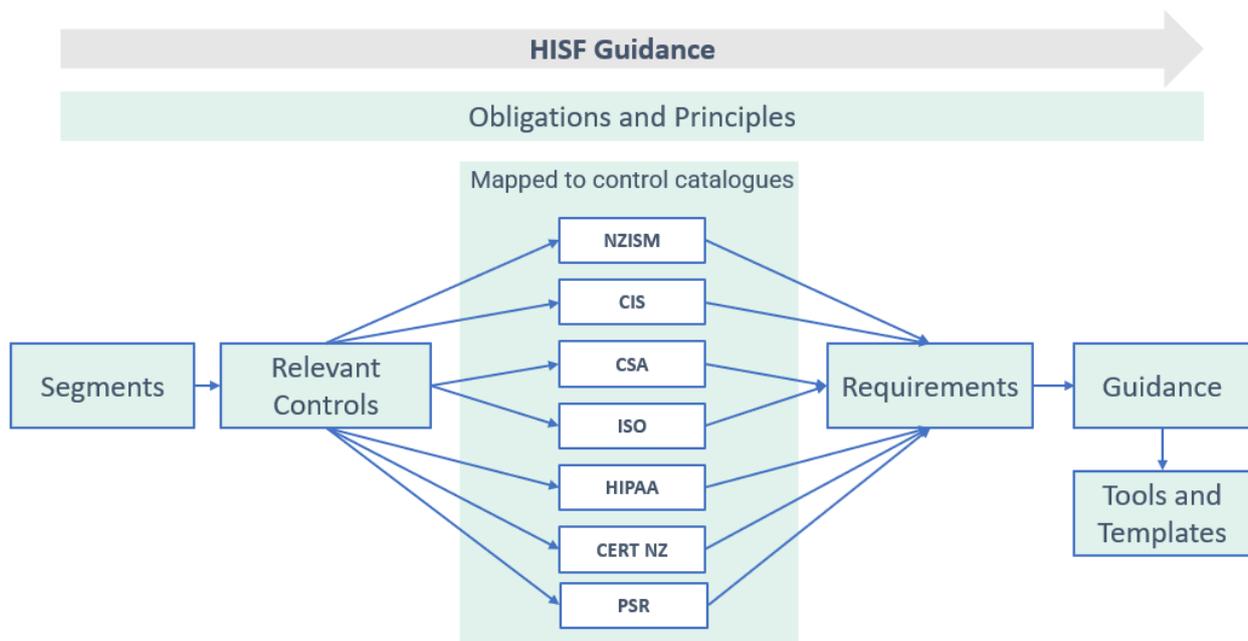


Figure 7: Control catalogues

The ‘Obligations’ and ‘Principles’ of our framework are overarching and apply to all health organisations within New Zealand.

‘Segments’ defined within the framework allow ‘Requirements’ to be tailored to varying levels of information security risk across segments. The requirements may change in response to changes in the threat environment and evolving maturity of a segment.

The control catalogues describe specific safeguards that can be implemented to meet our documented requirements. The control catalogues described in Figure 7 have been mapped to the requirements for each segment. An organisation can choose the relevant guidance for it to meet the specified requirements and overall obligations. As control catalogues are updated regularly, these are mapped rather than replicated within the framework. The mappings will be updated periodically.

‘Guidance’ is published in living documents that provide recommended capabilities and practices for organisations to meet the specified requirements and obligations.

To help the relevant segments based on their capabilities, standard operating procedures and workflows will be provided as part of ‘Tools and Templates’.

5.5 Cyber security requirements

The functional processes are underpinned by cyber security requirements. Requirements are high level statements which act as a checklist for the organisation to determine their compliance status with respect to the framework. They are also the statements which provide a foundation for a defence-in-depth protection.

The requirements are grouped according to the five functional processes with sub-categories as defined below. The sub-categories are an organising construct to group the more detailed requirements into areas of common practice and capability.

PLAN	IDENTIFY	PROTECT	DETECT	RESPOND
Acknowledge your obligations and put in place effective governance and plans to protect the security of health information.	Identify your information assets and understand the risks to information security and your organisation's capability to manage those risks (consistent with its risk management strategy and business needs)	Implement reasonable and appropriate safeguards covering people, process, procurement and technology risk	Continually test safeguards, detect threats, review and update plans and policies for emerging information security risks	Respond to information security incidents by activating business continuity, communication and information recovery procedures and by addressing identified vulnerabilities.
Establish governance	Identify risk	People risk	Test safeguards	Activate plans
Plans & Policies in place	Determine capability	Process risk	Review and update	Address vulnerabilities
		Technology risk	Monitor for events	Recover
		Procurement risk		

Figure 8: Five functional processes with sub-categories

The complete set of *proposed* requirements can be found in respective guidance documents for each segment.

The requirements presented in the respective guidance documents represent a common set of activities for managing cyber security risk. While it is not exhaustive, it is extensible, allowing organisations, sectors, and other entities to use subcategories and informative references that are cost-effective and efficient and that enable them to manage their cyber security risks.

5.6 Guidance

Guidance indicates the detailed level of implementation activities which the organisation needs to achieve control effectiveness. The implementation details are to be followed as appropriate to the organisation and system under consideration.

5.7 Tools and templates

A separate set of documents which are a combination of checklists and guides will be provided to the sector entities where there is limited or no documentation available to assist with the implementation activities of our framework. These documents can be tailored to the needs and requirements of the respective entities.

They also consist of a self-completion questionnaire using appropriate questions for organisations in each segment. Evidence confirming the implementation for each requirement may be used for reporting and planning of any cyber security initiatives.

6 References

When looking at each of the references below, ensure that the most recent version is identified and used:

- **Center for Internet Security (CIS):**
Designed to support the NIST framework developed in the USA and seen by many local information security practitioners to provide up-to-date guidance on international best practice.
- **CERT NZ Top Ten:**
Intended to help organisations decide what to spend the time and money on based on the assessment of 10 most critical controls.
- **Cloud Security Alliance (CSA) Cloud Controls Matrix:**
The Cloud Security Alliance controls are regarded as best-practice from organisations that have adopted as-a-service computing. Given the trajectory for the adoption of cloud computing services will continue to grow in the NZ health sector, the CSA controls provide international best-practice for controls in cloud computing environments.
- **Health Insurance Portability and Accountability Act (HIPAA) (US):**
US based federal law that required the creation of national standards (HIPAA Security Rule) to protect sensitive patient health information from being disclosed without the patient's consent or knowledge.
- **ISO 27001 Information Security Management Standard:**
An Information Security Standard that provides requirements for an information security management system (ISMS).
- **ISO 27002 Information Technology – Security Techniques – Code of practice for information security controls:**
An Information Security Standard that provides guidance on implementing ISO 27001:2022 Information Security Management System (ISMS).
- **ISO 27799 Health informatics – Information Security Management in health using ISO/IEC 27002:**
The health information specific version of the ISO 27002:2013 standard upon which the framework was initially based.
- **New Zealand Information Security Manual (NZISM):**
The dominant New Zealand information security framework provides the assurance of providing best-practice controls in a local context and reflects internationally accepted standards and controls.

- **Protective Security Requirements (PSR):**
Outlines the New Zealand government's expectations for security governance and for personnel, information and physical security.
- **Secure Controls Framework (SCF):**
Contains a collection of control catalogues compiled by an organisation called the Secure Controls Framework Council, LLC.
- **UK National Health Service assertions:**
A UK based Data Security and Protection Toolkit is an online self -assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards. It comprises of several assertions and evidence items.
- **US National Institute of Standards and Technology (NIST):**
A US based framework for improving critical infrastructure cyber security.

New Zealand Legislation

The following Acts of Parliament and Regulations have specific relevance to this standard. Readers must consider other Acts and Regulations and any amendments that are relevant to their own organisation when implementing or using this standard:

- Crimes Act 1961
- Electronic Transactions Act 2002
- Health Act 1956
- Health and Disability Commissioner (Code of Health and Disability Services Consumers' Rights) Regulations 1996
- Health Information Privacy Code 2020
- Health Practitioners Competence Assurance Act 2003
- Injury Prevention, Rehabilitation, and Compensation Act 2001
- Mental Health (Compulsory Assessment and Treatment) Act 1992
- Pae Ora (Healthy Futures) Act 2022
- Public Records Act 2005
- Privacy Act 2020

Appendix A – Glossary

Term	Definition
Health Information / Personal Health Information	<p>Health information is defined, broadly, in clause 4 of the Health Information Privacy Code 2020 and includes any information about the health of an identifiable individual, or any health or disability services provided to him or her. It also includes any information collected incidentally to providing services, such as appointment times and demographic data. It does not include anonymous data as it must be about an identifiable individual.</p> <p>This document focuses on the sharing of health information as defined above. For clarity, we have referred to any information about the health of an identifiable individual as personal health information.</p>
Information Security Architecture	<p>A description of the structure and behaviour for an enterprise's security processes, information security systems, personnel and organisational sub-units, showing their alignment with the enterprise's mission and strategic plans.</p>
NGO	<p>An NGO (Non-government organisation) is a non-profit, independent, community organisation that is not affiliated with central or local government, although they may receive financial and/or other support from the Government.</p>
Personnel	<p>Includes permanent, fixed term and temporary staff, contractors, consultants, volunteers, locums, and suppliers.</p>
PSR	<p>Protective Security Requirements (PSR) outlines the Government's expectations for managing personnel, physical and information security.</p>
Risk	<p>A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of:</p> <ul style="list-style-type: none"> • The adverse impacts that would arise if the circumstance or event occurs; and • The likelihood of occurrence.
Supplier	<p>Organisation or an individual that enters into an agreement with the acquirer for the supply of a product or service. This includes all suppliers in the supply chain, developers or manufacturers of</p>

Term	Definition
	systems, system components, or system services; systems integrators; suppliers; product resellers; and third-party partners.
User	A user is a person issued with a unique user ID who is authorised to use a computer system.