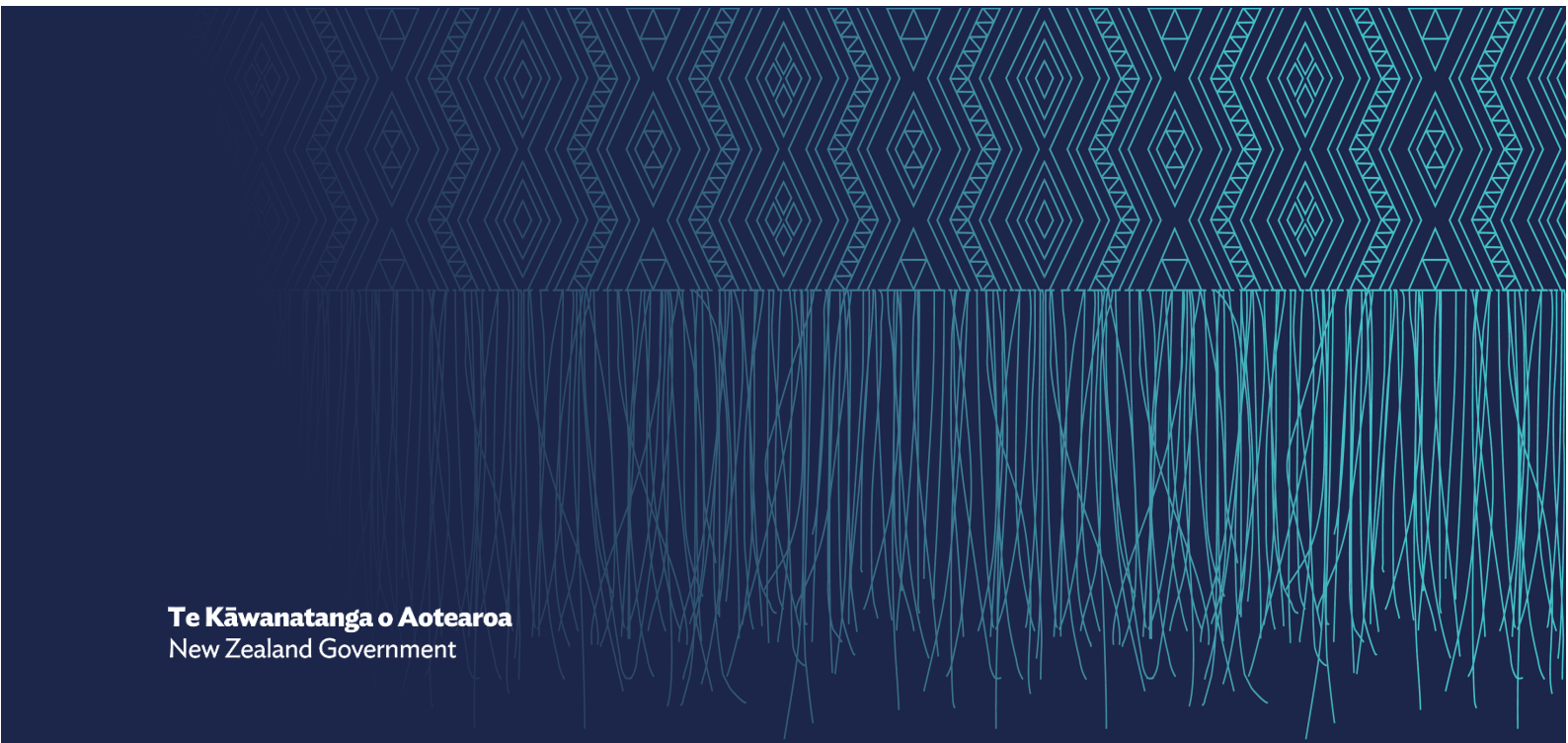
hiso Health Information Standards Organisation
PAEREWA PĀRONGO HAUORA

Te Whatu Ora
Health New Zealand

Health Information Security Framework Guidance for Medium to Large Organisations

HISO 10029.3:2023



Te Kāwanatanga o Aotearoa
New Zealand Government

Citation: Te Whatu Ora – Health New Zealand. 2023. *HISO 10029.3:2023 Health Information Security Framework – Guidance for Medium to Large Organisations*. Wellington: Te Whatu Ora – Health New Zealand.

Published in July 2023 by Te Whatu Ora – Health New Zealand
PO Box 793, Wellington 6140, New Zealand

ISBN 978-1-99-106732-6 (online)

Te Whatu Ora
Health New Zealand

This document is available at **tewhatuora.govt.nz**



This work is licensed under the Creative Commons Attribution 4.0 International licence. In essence, you are free to: share i.e., copy and redistribute the material in any medium or format; adapt i.e., 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

Purpose 3

Cyber security requirements for medium to large organisations 4

Requirements and guidance for medium to large organisations 9

Information security policy 9
Human resource security 13
Asset lifecycle security 22
Information security incident management 27
Business continuity and disaster recovery management 32
Supplier management 36
Cryptography 41
Identity and access management 43
Medical devices 50
Information Security Governance 55
Physical and environmental security 61
Remote working 68
Web security 70
Compliance 71
Cloud security 74
System acquisition, development and maintenance 82
Communications security 88
Risk management 91
Operations security 95
Information backups 95
Change management 98
Patch and vulnerability management 102
Configuration management 104
Capacity management 106
Endpoint security 106
Data leakage prevention 107
Logging and monitoring 108

Appendix A - Glossary 112

Purpose

This document is published as part of the Health Information Security Framework (HISF) to provide cyber security guidance for medium to large organisations in the health sector. This segment is defined as health organisations that fall into two or more of the following categories:

- organisations that may have presence at one or more geographic locations and supported by technology setup
- staffing of greater than 25 personnel
- manages a population of greater than 10,000
- may have some employees in-house managing IT that may be further supported by external IT and Security suppliers
- may be involved with health data collection from other regional healthcare providers and have data warehouses or similar setup
- may be involved in providing IT support to other healthcare providers
- may be involved with integrating or developing software systems or web applications in-house.

Implementation of the framework within medium to large organisations is a three-step process:

- understanding the published core framework document HISO 10029:2022 Health Information Security Framework
- reading the guidance and understanding the requirements as outlined in this document for medium to large organisations
- using HISF Tools and Templates, as well as other approved materials to meet the requirements outlined within this guidance document.

Start by reading the core framework document which provides foundational information on the segments, building blocks, functional processes, and principles of the framework, as well as the overall implementation approach. The requirements are linked to relevant national and international standards, as outlined in the core framework document.

This guidance document for medium to large organisations contains the detailed level of control implementation for all requirements grouped under the identified functional processes. These are recommendations and it is important to note that there could be other ways of implementation to meet the requirements, in addition to those in the guidance section.

You are welcome to use HISF Tools and Templates (e.g., checklists, templates, and forms) that are provided to help support, assess, implement and document your control effectiveness against the documented requirements.

Cyber security requirements for medium to large organisations

The list below contains cyber security requirements for medium to large organisations abbreviated as HML (HISF Medium to Large). The requirements are grouped according to the five functional processes as defined in section **5 HISF Framework** from the core framework document.

	PLAN
HML01	A clear information security policy, acceptable use policy, topic-specific policies and procedures are in place to maintain information security.
HML02	Security roles and responsibilities of personnel are included within job descriptions.
HML03	A breach of information security, including information by personnel, is considered a security policy violation. Consequences of a security policy violation leads to a disciplinary process.
HML04	Procedures for providing and revoking logical and physical access when personnel join, have a role change or leave the organisation are in place.
HML05	Asset management process(es) is in place.
HML06	Processes are in place for media equipment management, decommissioning and secure disposal.
HML07	An information security incident management process is in place.
HML08	Documented, approved, business continuity and disaster recovery management, operational resilience policies and procedures are established.
HML09	The information security requirements for managing the risks while a supplier is accessing information are to be identified and communicated.
HML10	Establish, document, approve, and implement rules to control physical and logical access to information and its assets.
HML11	Organisations are to include cyber security in procurement planning and decisions.
HML12	The organisation's Board or information security steering committee is accountable for organisation's information security governance.
HML13	A documented policy and supporting procedures for maintaining physical security within the organisation is in place.

HML14	A documented and approved procedure to remove papers and removable storage from easily accessible areas is implemented.
HML15	Organisations have planned maintenance of information via cloud services as per documented policies and agreements.
HML16	Information systems are securely designed, and appropriate controls are implemented.
HML17	A backup and recovery procedure is in place.
HML18	A documented process is in place for performing changes to new and existing systems or services related to information.
HML19	A documented process is in place for identifying vulnerabilities and updating patches on the organisation's systems, applications, tools, services etc.

IDENTIFY

HML20	Organisations, at a minimum, screen all personnel by verifying their identity, previous employment, applicable health professional qualifications and criminal backgrounds before confirmation of employment.
HML21	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.
HML22	There has been an assessment of information security training needs and a training plan is put in place.
HML23	Organisations are to have roles and responsibilities determined to carry out the incident management process.
HML24	Establish criteria for developing business continuity, disaster recovery, operational resilience strategies, and capabilities are to be determined based on disruption and impact to the organisation.
HML25	Suppliers are to be systematically evaluated, and their information security activities are reviewed before and after onboarding of their systems and services.
HML26	Vulnerability scanning on medical devices is only performed when they are in a test environment not connected for patient care.
HML27	Roles and responsibilities are defined and documented for planning, implementing, operating, assessing, and reporting on the organisation's information security requirements.
HML28	Organisations are to integrate information security into project management.
HML29	Relevant legal, regulatory and contractual requirements are identified and

	implemented.
HML30	A risk assessment methodology and cloud assurance activities that support the use of cloud technologies are in place.
HML31	Business and security requirements are identified, documented and approved when developing or acquiring applications.
HML32	Risk assessments are performed on new and existing systems and applications that manage information to understand the risks posed to the organisation while using them.
HML33	The proposed changes are to be analysed for potential security threats and their impact on the organisation.

PROTECT	
HML34	Information and associated assets are appropriately protected, used, and handled based on their importance.
HML35	In the event of a disruption or failure, critical information or services are identified, and measures are taken for the continuity of services.
HML36	The organisation's information security requirements are to be included in the agreements with the suppliers.
HML37	Rules for effective use of cryptography including encryption and key management are defined and implemented.
HML38	The complete lifecycle of the account(s) being used to access, process, or manage information and services is managed.
HML39	User accounts are authenticated and circumventing the authentication process is prevented.
HML40	Access to information and its associated assets is defined and authorised according to the business and security requirements and adhere to the organisation's identity and access management policy or procedures.
HML41	Organisations are to ensure that only authorised users, software components and services are provided with privileged access rights.
HML42	Access to source code, development tools, and software libraries are restricted, appropriately managed, and maintained.
HML43	Where possible, production and legacy medical devices are on a separate network.
HML44	All medical devices are maintained as per the latest updates from the manufacturers and current industry/regulatory standards.
HML45	Medical devices with patient information are digitally sanitised before their disposal or when they are being returned.
HML46	Metrics affecting the organisation's cyber security posture are regularly reported to the Board, and any decisions made are clearly documented.

HML47	Update, protect and maintain the devices installed as physical security safeguards including the utilities.
HML48	Secure areas of the organisation are protected from unauthorised personnel.
HML49	Secure mechanisms are available and supported by a documented policy or guidelines to connect to the organisation’s network.
HML50	Security controls are implemented if the organisation is developing the web applications to protect them from potential cyber-attacks.
HML51	The organisation's architectural strategy supports the adoption of cloud technologies.
HML52	Organisations are to make use of developed and configured APIs for secure transfer of information between different cloud components.
HML53	Organisations are to ensure that appropriate controls are implemented to protect information in a multi-tenant cloud environment.
HML54	Networks and network devices supporting the organisations’ systems and applications are to be securely managed.
HML55	The systems and applications that are used to process, store or transmit information are connected to a separate, dedicated network.
HML56	Backup copies of information, software and relevant systems are protected and maintained in accordance with the backup and recovery procedures.
HML57	Backups are tested for their restoration in accordance with the documented backup and recovery procedures. Organisations are able to access restored backups as well.
HML58	Organisations developing inhouse systems, applications or services are to maintain separate production and non-production environments.
HML59	Identified vulnerabilities or unpatched systems, services or applications within the organisation are properly identified, tracked and remediated.
HML60	Organisations have a standardised baseline configuration in place for new and existing systems, services and applications.
HML61	The capacity requirements for maintenance of information processing facilities, communication and environmental support during contingency operations are met.
HML62	Information, services, and applications on organisation systems and associated assets are protected against malware.

DETECT

HML63	The lessons learned from business continuity and disaster recovery testing are reflected in the established and implemented information security controls.
HML64	Medical devices are compliant with relevant standards, and the identified risks are documented within the medical device risk register.

HML65	Installed physical and environmental security mechanisms are monitored for potential security incidents.
HML66	Regular reviews are performed to confirm that the legal, regulatory, statutory, and contractual requirements are met.
HML67	Independent security reviews are defined and implemented before any new or major upgrades on systems are moved to the production environment.
HML68	Authorised personnel or teams are alerted upon unsuccessful or incomplete backups.
HML69	Organisations are to detect and prevent data leakage through the unauthorised disclosure and siphoning of information by individuals, systems or services.
HML70	The activities performed on the information processing systems, services and applications are logged and stored as per the organisation’s logging and auditing requirements.
HML71	Information processing systems, applications, devices, and services are synchronised to an approved time source.

RESPOND	
HML72	Breach of employment and supplier agreements are enforced.
HML73	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.
HML74	Evidence gathered as part of the incident management process is appropriately protected.
HML75	Organisations report all security incidents and near misses to the organisation's senior management or to the Board by a nominated Information Security Officer.

Requirements and guidance for medium to large organisations

Functional Process	Control Area	Requirement	Guidance
Information security policy Implementation of an information security policy ensures there is a continuous and effective management direction and support for the security of information (in accordance with their business, legal, regulatory, and contractual requirements). This section outlines the controls required for an effective policy which sets the expectations of all relevant stakeholders.			
Plan	Policies for information security	HML01: A clear information security policy, acceptable use policy, topic-specific policies and procedures are in place to maintain information security.	**Policies within organisations** An "information security policy" sets out the organisation's approach in managing its information security, while an "acceptable use policy" communicates the acceptable use of organisational information and its associated assets. These policies are to be defined, approved by top management, communicated to all relevant personnel, and reviewed periodically. **Information security policy** While documenting an information security policy to manage organisational information, consider: • scope and purpose of the policy • organisation's information security management structure • organisation's strategy, requirements, and security objectives • regulatory, legislative and contractual requirements • the current and projected information security risks and threats • definition of information security • information security objectives (or the framework for setting security objectives) • implementation of continual improvements related to information security • assignment of responsibilities for information security management • procedures for handling exemptions and exceptions • the needs and goals for information security • the legal and ethical responsibilities of health professionals to protect information • processes and procedures for notification of potential and actual information security incidents, including available channels for raising concerns relating to confidentiality, integrity and availability, without fear of blame or accusation • the identification of processes and systems that are vital in the health sector (i.e., where failure may lead to adverse patient impacts). In creating an information security policy document, organisations need to specifically consider the following factors, unique to the health sector: • the breadth of information • the rights and ethical responsibilities of personnel (as legislated), and as accepted by members of professional bodies • the rights of subjects of care, where applicable, to privacy and to access to their records

Functional Process	Control Area	Requirement	Guidance
			• the obligations of clinicians with respect to obtaining informational consent from subjects of care and maintaining the confidentiality of information • the legitimate needs of clinicians and organisations to overcome normal security protocols when healthcare priorities, often linked to the incapacity of certain subjects of care, necessitate such overrides • the obligations of the respective organisations, and of subjects of care, where healthcare is delivered on a “shared care” or “extended care” basis • the protocols and procedures to be applied to the sharing of information for the purposes of research and clinical trials • the arrangements for, and authority limits of, temporary staff (i.e., locums, students, “on-call” staff, charity personnel) • the impacts of information security measures on patient safety and performance of information systems. **Acceptable use policy** An acceptable use policy is to be established and communicated to anyone who uses or handles information and its associated assets. The acceptable use policy is to provide clear direction on how individuals are expected to use information and other associated assets. The acceptable use policy is to state: • purpose and scope of the policy • expected and unacceptable behaviours of individuals from an information security perspective • permitted and prohibited use of information and its associated assets • monitoring activities being performed by the organisation. Acceptable use procedures are to be drawn up for the full lifecycle of information, with appropriate controls for the type of information and its level of risk. While documenting, consider: • definition of the information to be protected, and what constitutes acceptable use • required access restrictions that support the protection of information • maintaining a record of authorised users • protection of temporary or permanent copies (e.g., print outs, USBs, local copies on laptops or desktops) to a level consistent with the protection of the original • storage of health assets (e.g., ultrasound devices, x-ray machines, CT scan devices, etc) in accordance with manufacturers’ specifications • clear marking of all copies of storage media (electronic or physical) for the attention of the authorised recipient • the responsibilities and actions of signatories to avoid unauthorised information disclosure, including what is permitted use • the right to audit and monitor activities that involve information • the process for notification and reporting of unauthorised disclosure or information leakage • authorisation for disposal of information and its associated assets, including agreed processes for disposal • the expected duration of an agreement (including cases where it may be necessary to maintain confidentiality indefinitely or until the associated information becomes publicly available) • guidance on when information or assets are to be returned or destroyed following the end of agreed use • the expected actions to be taken in the case of non-compliance.

Functional Process	Control Area	Requirement	Guidance
			The policy documents are to be made available to personnel electronically via a secure area on the organisation's intranet for reference purposes. Any changes made to these documents are to be approved by top management or similar groups within the organisation. **Topic-specific policies or procedures** The information security policy is supported by topic-specific policies as needed, to further mandate the implementation of additional information security controls. These policies are typically structured to address the needs of specific groups within the organisation or to cover defined security areas. Topic-specific policies are to be aligned with, and complementary to the information security policy of the organisations. In some organisations, the information security policy and topic-specific policies can be in a single document. Examples of such topic-specific policies or procedures include access control, asset management, backup, cryptography and key management, information management, management of technical vulnerabilities, network security, physical and environmental security, user endpoint devices, information security incident management, secure development, supplier management (as applicable), remote working, cloud security etc. Responsibility for development, review, and approval of specific policies are to be allocated to relevant authorised personnel, based on appropriate level of authority and technical competency. The review cycle is to include opportunities for improvement of these policies when there are changes in: • the organisation's business and security strategy • the organisation's technical environment • regulations, legislation, and contracts • information security risks and threat landscape • lessons learned from incidents. **Review of policies and procedures** The review of developed policies and procedures is to follow a set schedule, or be driven by the results of risk assessments, or reviewed when one policy is changed to maintain consistency. These revised policies are to be communicated to relevant personnel and interested parties in a way that is relevant, accessible, and understandable. Recipients of the policies are to acknowledge that they understand and agree to comply with the policies where applicable, and records of the acknowledgment are to be stored for documentation purposes. While reviewing the information security policies and topic-specific policies, consider: • the changing nature of the organisation's operations and the associated changes to the risk profile and risk management needs • the changes made to the IT infrastructure of the organisation, and the associated changes these bring to the organisation's risk profile • the changes identified in the external environment that similarly impact the organisation's risk profile • the latest guidance and recommendations from health professional associations (including the Privacy Commissioner regarding privacy protection of information, and other organisations such as Emergency Care Research institute (ECRI) for advice on managing medical devices, EU-MDCG Guidance on Cybersecurity for medical devices and other international standards • the results of legal cases tested in the courts, which have established or negated precedents or practices

Functional Process	Control Area	Requirement	Guidance
			• any challenges and issues regarding implementing the policy, as expressed by the organisation personnel, researchers, partner organisations and government bodies (e.g., the Privacy Commissioner) • reports on patient, personnel safety processes, information/records security and respective mitigation strategies to protect against the failure of information security measures.

Functional Process	Control Area	Requirement	Guidance
Human resource security Implementation of controls in this section ensures that personnel: • understand their responsibilities and are suitable for the roles for which they are considered • are aware of and fulfil their information security responsibilities • protect the organisation's interests when there is a change of role.			
Plan	Terms and conditions of employment	HML02: Security roles and responsibilities of personnel are included within job descriptions.	**Employment and contractual agreements** The individual employment agreement and contractual obligations for personnel are to consider the organisation's information security policy and relevant topic-specific policies. In addition, it may need to cover: • confidentiality or non-disclosure agreements (NDAs) that need to be signed by personnel prior to giving access to information and its associated assets • legal responsibilities and rights (e.g., regarding copyright and privacy laws or data protection legislation) • responsibilities for management and handling of information, its associated assets, information processing facilities, and services handled by the personnel • responsibilities for reporting breaches of information security or patient information to the incident management team within a specific timeframe • actions to be taken if personnel disregard the organisation's security requirements. **Roles and responsibilities** Information security roles and responsibilities are communicated to candidates during the pre-employment process and the organisation ensures that personnel agree to them before being onboarded. These terms and conditions are appropriate for their role and the level of access they will have to the organisation's assets associated with information systems and services including and not limited to patient information (as applicable). The terms and conditions concerning information security are reviewed when laws, regulations, the information security policy, or topic-specific policies change.
Plan	Terms and conditions of employment	HML03: A breach of information security, including information by personnel, is considered a security policy violation. Consequences of a security policy violation leads to a disciplinary process.	**Disciplinary process** Disciplinary processes, with respect to breaches of information, are to follow documented and approved procedures, made available to the subject(s) of the disciplinary process. The processes are to comply with the agreements reached between the organisation and professional union bodies or as applicable. The disciplinary process is not to be initiated without prior verification that an information security policy violation or breach of information has occurred. A formal disciplinary process is to consider: • the nature (who, what, when, and how) and gravity of the breach and its consequences • whether the offence was intentional (malicious) or unintentional (accidental) • whether or not this is a first or repeated offence • whether or not the violator was properly trained. The response is to consider relevant legal, statutory, regulatory, contractual, business and security requirements (as well as any other factors required). The disciplinary process is to be used as a deterrent to prevent personnel and other relevant parties from violating the information security policy, topic-specific policies, and procedures for

Functional Process	Control Area	Requirement	Guidance
			information security. Deliberate information security policy violations can require immediate action. Where possible, the identity of individuals subject to disciplinary action is to be protected.
Plan	Onboarding, offboarding and role change	HML04: Procedures for providing and revoking logical and physical access when personnel join, have a role change or leave the organisation are in place.	**Documented procedures** Documented user access creation, modification, and deletion procedures clearly identify whether personnel: • have access to organisational and customer information • have the right access to information based on their roles and responsibilities • have both physical and logical access disabled while on extended leave (e.g., sick leave, maternity leave, extended leave) • have access to the premise removed as soon as possible following a temporary or permanent departure. **Onboarding and offboarding** Assigning or revoking access to information and its associated assets (e.g., laptops, mobile devices, access cards, etc.) is usually a multi-step procedure: • confirming the business and security requirements for personnel to whom access is being provided • verifying the relevant qualifications before access allocation • configuring and activating the access (including configuration and initial setup of related authentication services) • providing or revoking specific access rights to personnel, based on appropriate authorisation or entitlement decisions. The process for assigning or revoking physical and logical access rights granted to the organisation's personnel are to consider: • obtaining authorisation from the business owner of the information and its associated assets for their use • business, security requirements and the organisation's topic-specific policy or procedure and rules on access control • segregation of duties (including segregating the roles of approval and implementation of access rights to avoid any conflict or overlap) • ensuring access rights are removed when someone no longer needs access to information and its associated assets (in particular ensuring access rights of users who have left the organisation are removed in a timely fashion) • providing temporary access rights for a limited period and revoking them at the expiration date • verifying that the level of access granted aligns with the topic-specific policies or procedures on access control and is consistent with other information security requirements such as segregation of duties • ensuring that access rights are activated only after authorisation procedures are successfully completed • maintaining a central record of access rights (covering both information and assets) granted to a user identifier (ID, logical or physical) • modifying access rights of users who have changed roles or jobs • removing or adjusting physical and logical access rights (which may include removal, revocation or replacement of keys, authentication information, identification cards or subscriptions) • maintaining a record of changes to users' logical and physical access rights. Special consideration needs to be given to users who will reasonably be expected to provide emergency care, as they may need access to information in emergency situations, where a subject of care may be unable to communicate consent. There may be temporary personnel within the organisation who have retained their access privileges after completion of their internship, contracts, etc. The termination of the access rights of such personnel needs to be carefully managed, as in healthcare, many transactions often take place well after the time of care (e.g., the sign-

Functional Process	Control Area	Requirement	Guidance
			off of medical transcripts). This can significantly complicate the process of removing access rights in a timely fashion, and these transactions are to be considered when designing and implementing relevant procedures. **Access reviews** Regular reviews of physical and logical access rights are to consider: • users' access rights after any change of employment within the same organisation (e.g., role change, promotion, demotion) or termination of employment • need-to-know and least privilege access control principles • authorisations for privileged access rights. A user's access rights to information and its associated assets are to be reviewed before any change or termination of employment, and subsequently adjusted or removed based on risk factors such as: • whether the termination or change is initiated by the user or by management and the reason for termination • the current responsibilities of the user • the value of the assets currently accessible. Organisations are to seriously consider immediate termination of access rights following a resignation notice, notice of dismissal, etc. where there is an increased risk from continued access.
Identify	Terms and conditions of employment	HML20: Organisations, at a minimum, screen all personnel by verifying their identity, previous employment, applicable health professional qualifications and criminal backgrounds before confirmation of employment.	**Hiring process** Where personnel are hired directly by the organisation (or contracted through suppliers or through recruitment agencies), a documented and approved screening process is to be followed before providing access to an organisation's information and infrastructure. For individuals contracted through suppliers, screening requirements are included in the contractual agreements between the organisation and the suppliers. Information on all candidates being considered for positions within the organisation are to be collected (where applicable) and handled following information management practices. Where an individual is expected to process information, a minimum of the following is to be verified at the time of job application: • identity • previous employment • professional qualifications. Verification is to consider all relevant information protection, and employment-based legislation and where permitted, include: • availability of satisfactory references (e.g., professional, and personal references) • verification (for completeness and accuracy) of the applicant's CV • confirmation of claimed academic and professional qualifications • independent identity verification (e.g., passport or driver's license) • review of criminal records (e.g., Ministry of Justice checks) • more detailed verification where required (such as a credit review if the candidate takes on a financial role). When an individual is hired for a specific information security role, the organisation is to make sure the candidate: • has the necessary competence to perform the security role • can be appropriately trusted, especially if the role is critical for the organisation • clearly understand the expectations towards the security role and their obligations to the organisation.

Functional Process	Control Area	Requirement	Guidance
			Where a role, either through appointment or subsequent promotion, involves the person having a change of access to information (e.g., needing to modify or remove access to information), the organisation is to consider more detailed verifications relative to the new role and its responsibilities. Procedures are to define criteria and the limitations for verification reviews (i.e., who is eligible to screen people and how, when, and why verification reviews are carried out). In situations where verification cannot be completed in a timely manner, mitigating controls are to be implemented until the review has been finished, for example: • delayed onboarding • delayed deployment of corporate assets • onboarding with limited access • potential termination of employment. Verification checks are to be repeated periodically at a minimum of once every 3 years (and more frequently for roles modifying or removing information to confirm ongoing suitability of access), depending on the criticality of the role. Background checks however might have already been carried out as part of a health professional's accreditation. **Code of conduct** A code of conduct can be used to state information security responsibilities regarding confidentiality, information protection, ethics, appropriate use of the organisation's information and its associated assets, as well as other practices expected by the organisation. **Supplier staff** An external party, with which supplier personnel are associated, will be required to enter into contractual agreements on behalf of the contracted individual. Both the supplier and their representatives are expected to sign the organisation's code of conduct and acceptable use policy as part of a master agreement. Supplier staff are to also be monitored regularly to ensure ongoing suitability for the work required. If the supplier organisation is not a legal entity and does not have employees, the equivalent of a contractual agreement and terms and conditions can be considered in line with the guidance of this control. Assessing the risks from the supplier staff is especially important when they have offshore interests or when an individual provides their services for the supplier organisation from a different legal jurisdiction.

Functional Process	Control Area	Requirement	Guidance
Identify	Roles and responsibilities	HML21: 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.	**Roles and responsibilities** Organisations are to have documented support of management (including statements of commitment to the importance of information security and recognition of its benefits) before trying to adopt the HISF, as this is essential for success. Accountability and coordination can only be maintained over the long term if the organisation has an explicit information security management infrastructure. Whatever structure is adopted, it is essential that it's designed and structured to facilitate access by subjects of care (e.g., to make requests to obtain information), to facilitate reporting within the organisational structure, and to ensure timely delivery of information. Allocation of information security roles and responsibilities is to be done in accordance with the information security policy and topic-specific policies and procedures. The organisation is to define and manage responsibilities for: • protection of information and its associated assets • carrying out specific processes for information security • security risk management activities (particularly acceptance of residual risks i.e., who are the risk owners) • all personnel using information and its associated assets. These responsibilities are to be supplemented, where necessary, with more detailed guidance for specific sites and facilities where information is processed. Personnel with allocated information security responsibilities can assign security tasks to others, however they remain ultimately accountable and are to ensure any delegated tasks have been correctly performed. Each security (information, personal, physical) area for which personnel are responsible and the relative authorisation levels are to be defined, documented communicated and reviewed periodically. Personnel who take on a specific security role is to have the required competency, knowledge and skills, and be supported to keep up to date with any changes to the role needed to fulfil the organisation's responsibilities. An appropriate group is to be appointed to oversee and direct information security. What constitutes "appropriate" in this context varies among organisations and will also vary across the spectrum of healthcare. Structuring the group may be challenging, with many stakeholders' views to be accommodated and many regulatory obligations to be met. While the functions of the group cannot be devolved or dispersed without losing effectiveness, it is not necessary that giving responsibility to a chosen group requires the creation of "yet another committee". It is often better to extend the focus of an existing committee, such as one that addresses risks or that undertakes information governance. Established roles will need to encompass the full range of information assurance and information governance functions related to health, as well as representatives of the different user communities and representatives of the key support functions. Representatives of Internal Audit and Human Resources are also typically present. The central nature of information security within information governance makes the positioning of the group within the information governance structure a sensible arrangement, but only if the latter group is, in turn, linked to the clinical governance structure. Organisations are to publicise the scope statement widely internally, then review it

Functional Process	Control Area	Requirement	Guidance
			to ensure it is adopted by the organisation's information, clinical, non-clinical and corporate governance groups. Clinical governance deals with patient safety issues and these are often closely related to information security issues to which information governance is to attend. Taking an information governance approach underscores the critical nature of information security and allows an integrated process, with risk analysis input, that directly feeds clinical governance. The removal of the "silo" mentality separating information security, data protection, freedom of information, etc., eliminates duplicated costs and enhances process integrity. Many organisations appoint an information security manager to take overall responsibility for the development and implementation of information security and to support the identification of risks and mitigating controls. However, responsibility for resourcing and implementing the controls often remains with respective managers. One common practice is to appoint an owner for each asset who then becomes responsible for its day-to-day protection (i.e., business owner). Depending on the size and resourcing of the organisation, information security can be covered by dedicated roles or duties, carried out in addition to existing roles. **Chief Information Security Officer (CISO)** The organisation's appointed CISO is to ensure that security of information is managed at the executive level. This role: • is accountable for implementation of information security practices at various departments within the organisation • ensures the organisation's security objectives are aligned to the implementation practices • provides strategic guidance • publicises the scope statement widely internally, reviews it, and ensures it is adopted by the organisation's information, clinical, non-clinical and corporate governance groups • ensures that the organisation complies with relevant legislation, regulatory, contractual requirements and industry best practices • is accountable for the development and maintenance of an information security awareness and training programme • oversees management of information security personnel within the organisation • advises on ICT projects • provides recommendations on the status of any residual risks identified • coordinates with external information security resources so that a consistent information security approach is maintained within the organisation. **Information Security Officer or Manager** The organisation's information security officer is to, among other duties, report to the senior management. The officer is responsible for collating, publishing, and commenting on the reports received by the senior management. **Internal Auditor** Establishes a security baseline to which future audits can be conformed to: • help comply with the organisation's security policies • help comply with external regulatory and legal requirements

Functional Process	Control Area	Requirement	Guidance
			• determine if and how security is adequate • conduct regular audits to help the organisation meet their security and business objectives (recommended every quarter).
Identify	Training requirements	HML22: There has been an assessment of information security training needs and a training plan is put in place.	An information security awareness, education, and training programme are to be established, in line with the organisation's information security policy, topic-specific policies, and relevant procedures. Information security awareness, education and training is to take place periodically. This can initially apply to new personnel or those who transfer to new positions or roles with substantially different information security requirements. Personnel's understanding is to be assessed at the end of an awareness, education, or training activity to test their knowledge and the effectiveness of the activity. **Security awareness programme** An information security awareness programme is to make personnel aware of their responsibilities and what they are required to do, including specific responsibilities for different roles. The activities in the awareness programme are to be repeated periodically, so that activities are reinforced while also including new joiners. Factual information security incidents can also be used to help develop future awareness activities. The awareness programme is to include multiple activities across an appropriate range of channels (including physical or virtual channels such as campaigns, booklets, posters, newsletters, websites, information sessions, briefings, e-learning modules, and e-mails). The programme is to cover: • management's commitment to information security and protecting information throughout the organisation • familiarity and compliance needs concerning applicable information security rules and obligations, considering information security policy and topic-specific policies, procedures, standards, guidelines, statutes, regulations, contracts, and agreements • personal accountability and general responsibilities in securing or protecting information • basic information security procedures (e.g., information security event reporting) and baseline controls (e.g., password security, multi-factor authentication) • contact points and resources for additional information and advice on information security, including further awareness materials. When composing an awareness programme, it is important not only to focus on the 'what' and 'how', but also the 'why' (when possible). Information security awareness, education and training can be part of, or conducted in collaboration with, other activities (e.g., general information management, ICT, security, privacy, or safety training). **Education and training** Organisations are to identify, prepare, and implement an appropriate training plan for teams whose roles require specific skills and expertise (e.g., biomedical and technical teams need the skills for configuring and maintaining the required security level for biomedical devices, corporate devices, systems, applications, and services related to healthcare).

Functional Process	Control Area	Requirement	Guidance
			If there are required skills that have been identified for a role or team that are not present, the organisation is to acquire them. A review of required skills is to be performed periodically (or at least every year). The education and training programme is to consider different methods of learning (e.g., lectures, self-studies, or being mentored by expert personnel or consultants through on-the-job training). Individuals can also keep their knowledge up to date by subscribing to newsletters and magazines, or attending conferences and events aimed at healthcare, technical and/or professional development. The information security awareness training is to cover: • how to identify and report a cyber security incident • how to recognise social engineering attacks • what is a malware and what constitutes its behaviour and how to recognise one • authentication best practices • information lifecycle and data handling best practices • causes of unintentional data exposure • how to identify and report if their assets are missing security updates • connecting to and transmitting data over insecure networks. **Leadership roles** The organisation's risk profile and threat landscape (identified as part of the Business Impact Assessment, which is further explained in Business Continuity and Disaster Recovery Management domain) are to be included as part of training for those in senior roles, based on their roles and responsibilities. Additional training, if required, is to be provided so that the organisation's risks are maintained and managed at least annually.
Respond	Terms and conditions of employment	HML72: Breach of employment and supplier agreements are enforced.	**Agreement breach governance** Security responsibilities that are applicable during or after termination of employment or contractual or supplier agreements are to be defined, enforced, and communicated. In healthcare, many personnel (i.e., doctors, and nurses) commonly progress through training programmes and other "rotations" where their required access rights can change. The process for managing change of employment is to define which information security responsibilities and duties remain valid or need to be added after the change of role. This may include confidentiality of information, intellectual property and other knowledge obtained, as well as responsibilities contained within any other confidentiality agreement. Previous rights that are no longer required are to be removed and processed in the same way as for personnel who are leaving the organisation including returning of the organisation's assets. Changes are to be implemented in line and in combination with the termination of the current responsibility or employment, and the initiation of the new responsibility or employment. Information security roles and responsibilities held by any personnel who leaves or changes job roles, is to be identified and transferred to another individual. A process is to be established to communicate any changes (including operating procedures) to relevant personnel and contact persons (e.g., suppliers).

Functional Process	Control Area	Requirement	Guidance
			The process for the termination or change of employment is to also be applied to suppliers when a termination occurs of their personnel, the contract, the job with the organisation, or when there is a change of the job within the organisation. Typically, the human resource function is responsible for the overall termination process and works together with the supervising manager of the person transitioning to manage the information security aspects of the procedure. In the case of personnel provided through an external party (e.g., through a supplier), this termination process is undertaken by the external party in accordance with the existing contract between the organisation and the external party.

Functional Process	Control Area	Requirement	Guidance
Asset lifecycle security Implementation of controls in this section ensures that assets (both corporate devices and medical devices): • are identified to define respective protection responsibilities, usage, and handling • prevent unauthorised disclosure, modification, removal, or destruction of information stored on these assets.			
Plan	Information and associated assets	HML05: Asset management process(es) is in place.	**Asset management process** Organisations are to manage a documented and approved process to procure, maintain and disposal of assets which includes: • procurement of computing and health devices (as applicable) from a known, authorised supplier and via approved procedures • performing relevant due diligence activities • accounting for all information assets (i.e., maintain an inventory of such assets) • having a designated custodian of information assets • having rules identified, documented, and implemented for acceptable use of these assets • classifying all identified assets and identify their protection requirement • securing the sanitisation and destruction process before disposal. An inventory of information and its associated assets are to be kept accurate, up to date, consistent and aligned with other inventories. Options for ensuring accuracy of an inventory of information and its associated assets include: • conducting periodic reviews of identified information and its associated assets against the asset inventory • automatically enforcing an inventory update in the process of installing, changing, or removing an asset. Note: The location of an asset is to be included in the inventory as appropriate. Devices that record or report data (e.g., medical devices) may require special security considerations depending on the environment they operate in (including potential electromagnetic emissions that may occur during their operation). Such devices are to be uniquely identified. Ensuring that inventories are maintained by relevant functions, a set of dynamic inventories, including inventories for information assets, hardware, software, virtual machines (VMs), facilities, personnel, competencies, capabilities, and records can be created. For identified information, software and endpoint devices, ownership and maintenance of the asset is to be assigned to an individual or a group. A process to ensure timely allocation of asset ownership is to be implemented. Ownership is assigned when assets are created or transferred into the organisation. Asset ownership is to be reassigned as necessary when the current asset owner leaves or changes job role. **Ownership of assets** The organisation, when identifying information assets, is to determine their importance based on the level of information security and its owner. Documentation is to be maintained for dedicated (e.g. medical devices, corporate devices etc) or existing inventories.

Functional Process	Control Area	Requirement	Guidance
			Assets include all information assets and computing devices that is captured, processed, transferred, stored, or recalled by the organisation and all devices and systems owned or used by the organisation for the capturing, processing, transferring, storing or recalling of information. This includes all on and off premise devices, and service platforms used for these activities including specialist medical devices. The inventory of these information assets is to: • be accurate, up to date, consistent, reviewed periodically and aligned with other inventories • all information assets containing information are to be labelled, classified and regularly tracked • include rules for maintaining the currency of assets (e.g., the currency of a drug database) and the integrity of these assets (e.g., the functional integrity of medical devices that record or report data). While many information assets can be owned by organisations in the conventional sense, health professionals are often viewed as custodians or trustees in relation to personal information. The asset owner is responsible for the proper management of an asset over the whole asset life cycle, ensuring that: • information and its associated assets are inventoried • information and its associated assets are appropriately classified and protected • components supporting technology assets are listed and linked (i.e., database, storage, software components and sub-components) • requirements for the acceptable use of information and its associated assets are established • access restrictions are effective and reviewed periodically • information and its associated assets, when wiped, de-provisioned, disposed, destroyed or ported to another location, are handled in a secure manner, and updated in the inventory • they are involved in the continuous identification and management of risks associated with the asset(s) assigned • they support personnel who have the roles and responsibilities in managing information within the asset. **Leased devices** It can be the case that the assets concerned do not directly belong to the organisation, such as loaned devices, leased devices, and public cloud services. The use of third-party assets in conjunction with the organisation assets (e.g., through agreements with cloud service providers or mobile device management (MDM)). Care is to be taken when a collaborative working environment is used.
Plan	Media equipment management, decommissioning and disposal	HML06: Processes are in place for media equipment management, decommissioning and secure disposal.	**Documented processes** Organisations are to maintain a documented and approved process to allow authorised individuals to move and remove assets (e.g., network devices, servers, etc) from the premise. An approval process is to be in place for taking these assets out of the organisation for repairs or disposal activities. This could also be in the form of an overarching approval for a group of specific roles within the organisation, rather than on an individual level. If updating the asset register is not automated, it is to be updated periodically and signed off by a reviewer when there is a change (this is not applicable to personnel owned laptops, and mobile phones). If any of the changes result in an infrastructure change, documented and approved change management processes are to be followed.

Functional Process	Control Area	Requirement	Guidance
			Asset register Organisations are to maintain a register of the devices or assets which are decommissioned or destroyed, along with evidence of secure disposal or destruction. The asset owner is to be notified of incomplete and complete sanitisation reports before decommissioning to update the register. **Removable storage media** Organisations processing or managing or storing information on removable storage media are to consider: • establishing a topic-specific policy or procedure and communicating this to anyone who uses or handles removable storage media • requiring authorisation for servers, network devices, medical devices, etc to be removed from the organisation and keeping a record to maintain an audit trail • storing all storage media in a safe, secure environment that protects against environmental threats (such as heat, moisture, humidity, electronic field, or ageing), in accordance with manufacturers' specifications • using cryptographic techniques to achieve confidentiality and integrity when protecting information on removable storage media • transferring information to separate storage media and storing multiple copies to mitigate the risk of it degrading, coincidental damage or loss, becoming unreadable while still needed • registration and labelling of removable storage media to limit the chance of loss • disabling storage media ports (e.g., secure digital (SD) card slots and universal serial bus (USB) ports) on medical devices, unless there is a documented organisation need for their use • monitoring the transfer of information to removable storage media • securely disposing of any storage devices, drums or cartridges with memory chips removed during maintenance or servicing • secure transportation to reduce vulnerability to unauthorised access, misuse, or corruption during physical transport (i.e., when sending storage media via the postal service or courier). **Secure reuse or disposal** Improper reuse or disposal of media containing information continues to be a source of serious breaches of patient confidentiality, integrity and availability of information. It is important to note that this control is to be applied prior to the repair or disposal of any associated equipment. Procedures for the secure reuse or disposal of storage media containing information including patient personally identifiable information are to be established to minimise the risk of information leakage to unauthorised parties (in accordance with Public Records Act 2005). Before reuse, disposal, or recycling of media, consider: • if storage media containing information need to be reused within or outside the organisation, the information residing on the media is to be securely wiped, or formatted appropriately before reuse • disposing of storage media securely when not needed anymore (e.g., by destroying, shredding, or securely deleting the content) • having procedures in place to identify items that require secure disposal • if collection and disposal services for storage media are being outsourced, selecting a suitable external party supplier with adequate controls and experience • logging the disposal of medical devices or devices on which information is stored to maintain an audit trail

Functional Process	Control Area	Requirement	Guidance
			• a secure disposal certificate stating that agreed procedures were followed is to be provided to the requesting organisation and maintained for reference purposes. This is also applicable for medical equipment • when accumulating storage media for disposal, be aware of the aggregation effect, which can cause information to become sensitive and/or identifiable • a risk assessment is performed on damaged devices to determine whether the items are to be physically destroyed rather than sent for repair or discarded. When information on storage media is not encrypted, additional physical protection of the storage media is to be considered that match the protection requirement for the information that is similarly classified.
Protect	Information and associated assets	HML34: Information and associated assets are appropriately protected, used, and handled based on their importance.	**Critical systems and services** The criticality and importance of information assets to the organisation are to be assessed. An assessment to identify the critical systems and services can also be performed to identify and reduce the risks from physical and environmental threats, and from unauthorised access and damage. A minimum of the following guidelines is to be considered to protect assets: • carefully positioning equipment and information processing facilities to minimise unnecessary access into certain work areas and to avoid unauthorised access • adopting controls to minimise the risk of potential physical and environmental threats (e.g., theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation, or vandalism) • establishing guidelines for eating, drinking, and smoking in proximity to information processing facilities • monitoring environmental conditions (i.e., temperature and humidity), which can adversely affect information processing facilities • applying lightning protection to all buildings, and fitting lightning protection filters to all incoming power and communications lines • the use of special protection methods (i.e., keyboard membranes) for equipment in healthcare environments • protecting equipment processing information to minimise the risk of information leakage • physically separating information processing facilities managed by the organisation from those not managed by the organisation • ensuring risk assessments address the potential impacts to information which is stored, processed or transmitted by assets • maintaining a log that defines the chain of custody for equipment being transferred between sites • implementing location tracking for equipment being transferred and a remote wiping capability to preserve the confidentiality of information. Organisations are to situate any workstations with access to information in a way that prevents unintended viewing or access by subjects of care and the public. Medical devices that record or report data may also require special security considerations depending on the environment in which they operate, and any electromagnetic emissions that may occur during their operation. Organisations are to ensure there are siting and protection guidelines for this equipment to minimise exposure to such emissions. **Protection of devices** Organisations are to ensure that all information and its associated assets are: • encrypted while its media are in transit, or • physically and logically protected from theft while its media are in transit

Functional Process	Control Area	Requirement	Guidance
			• secured by a remote wiping capability to lessen the risk of theft. **Physical security of devices** Physical security is the implementation of safeguards to ensure protection of physical assets used to store, process, or transmit information from actions or events that can cause damage to the organisation and its assets. This protection can also be from internal or external intruders that threaten data security. If information is being transferred using external media devices (e.g., USBs, hard drives,) from one location to another, it is recommended that the device and information within the device is encrypted, and password protected. Default logins on operating systems or hardware are to be either encrypted, changed or disabled so that usernames and passwords are not easily guessed by hackers. Medical devices are an exception to this rule if the option is not available.
Respond	Information and associated assets	HML73: 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.	**Information security requirements** Personnel accessing information and its associated assets are to be made aware of all relevant information security requirements. They are to be responsible for the use of any information processing facilities. **Documented procedures** The topic-specific policy or procedures on acceptable use are to provide clear direction on how individuals are expected to use information and its associated assets. The topic-specific policy or procedure is to state: • expected and unacceptable behaviours of individuals from an information security perspective • permitted and prohibited use of information and its associated assets • monitoring activities being performed by the organisation • disciplinary actions to be enforced if there is a breach in the policy. Acceptable use procedures are to be drawn up covering the full information lifecycle (in accordance with its protection requirements including potential risks) while considering: • access restrictions that support protection of information • maintenance of a record of authorised users of information and its associated assets • protection of temporary or permanent copies of information (to a level consistent with the protection requirements of the original information) • storage of assets associated with information (in accordance with manufacturers' specifications and the information protection requirement) • clear markings of all copies of storage media (electronic or physical) for the attention of the authorised recipient • authorisation of disposal of information and its associated assets, including the supported deletion method(s). •

Functional Process	Control Area	Requirement	Guidance
Information security incident management Implementation of controls in this section ensures that: • an effective and efficient response to information security incidents, to reduce likelihood and consequences of recurrence • consistent and effective management of evidence related to the incident(s) for the purposes of disciplinary and legal actions.			
Plan	Planning and preparation	HML07: An information security incident management process is in place.	**Information security incident management** The objectives for information security incident management are to be agreed with the management, and it is to be ensured that those responsible for information security incident management understand the organisation's priorities for handling incidents (including resolution timeframe based on potential consequences and severity). Incident management procedures are to be implemented to meet these objectives and priorities. **Reporting an information security incident** All individuals are to be made aware of their responsibility to report any information security events as quickly as possible to prevent or minimise potential impact. They are to be aware of the procedure for reporting information security events (including incidents, potential breaches, and vulnerabilities) and the point of contact for reporting these. The reporting mechanism is to be easy, accessible, and available. Situations to be considered for information security event reporting include: • ineffective information security controls • breach of information confidentiality, integrity, or availability expectations • human errors (e.g., leaving documents containing information at the printers) • non-compliance with the information security policy, topic-specific policies, procedures, or applicable standards • breaches of physical security measures • system changes that have not gone through the change management process • malfunctions or other abnormal behaviour of software or hardware • access violations • software or hardware vulnerabilities (including the systems that have not been updated before becoming fully operational) • suspected malware infection. Organisational personnel are to be advised not to attempt to prove suspected information security vulnerabilities. Testing vulnerabilities can be interpreted as a potential misuse of the system and can also cause damage to the information system or the service (and it can corrupt or obscure digital evidence). Ultimately, this can result in legal liability for the individual performing the testing. **Testing of the information security incident management process** Regular table-top exercises are to be conducted with relevant teams to prepare for information security incidents, while including the following in a response plan: • establish a common method for reporting information security events including identifying a point of contact and their backups • roles and responsibilities for carrying out the incident management procedures. These are to be effectively communicated to the relevant internal and external stakeholders

Functional Process	Control Area	Requirement	Guidance
			• identification of critical IT suppliers with whom the incident response plan is to be tested periodically on a rotational basis • incident management procedures including administration, detection, triage, prioritisation, analysis, communication, event co-ordination activities so that the organisation's priorities for handling information security incidents are met (including resolution timeframe based on potential consequences, severity and the business impact analysis performed) • reporting procedures - including the use of incident forms, feedback processes, creation of incident reports, post incident review and external reporting obligations (specifically with regards to subjects of care if information may have been unintentionally disclosed) • prioritisation/escalation protocols providing an effective escalation path for incidents, so that crisis management and business continuity management plans can be invoked in the right circumstances and at the right time • methods to collect and preserve incident-related audit logs and other relevant evidence. The documented incident response plan is tested at least annually and maintained to ensure it is effective and can be implemented efficiently and effectively when needed. Necessary modifications to the plan are to be made based on the test results or post an incident review. **Information security incident management plan** The organisation's management are to ensure that an information security incident management plan is created considering different scenarios, and procedures are developed and implemented for the following activities: • regular table-top exercises to ensure teams are well equipped with the knowledge and tools to handle incidents when they occur • evaluation of information security events (according to criteria for what constitutes an information security incident) • monitoring, detecting, classifying, analysing, and reporting • managing information security incidents through to conclusion, including response and escalation, according to the type and the category of the incident, possible activation of crisis management and activation of continuity plans, controlled recovery from an incident, and communication to internal and external interested parties • co-ordination with internal and external interested parties such as authorities, external interest groups and forums, suppliers, and clients • logging incident management activities • acceptable method(s) of handling of evidence • root cause analysis or post-mortem procedures • identification of lessons learned and any required improvements to the incident management procedures or information security controls • documented policies and procedures are regularly reviewed (at least annually or upon a major security incident), approved, communicated, evaluated, and maintained. These plans are to be tested periodically (not necessarily in production environments), reviewed, and stored for reference purposes. A detailed information security incident management plan is to include reporting procedures and the way the incidents are responded to. The reporting procedures are to include:

Functional Process	Control Area	Requirement	Guidance
			• actions to be taken in case of an information security event (e.g., noting all relevant details immediately such as malfunction and messages on screen, immediately reporting to the point of contact, and only performing coordinated actions) • use of incident forms to support personnel to perform all necessary actions when reporting information security incidents • suitable feedback processes to ensure those persons reporting information security events are notified, to the extent possible, of outcomes after the issue has been addressed and closed • creation of incident reports. Any external requirements on reporting of incidents to relevant interested parties within the defined timeframe (e.g., breach notification requirements to Te Whatu Ora, National Cyber Security Centre (NCSC), CertNZ, cyber insurance providers as applicable) are to be considered when implementing incident management procedures. **Communication during an information security incident** In case of an event, the organisation is to also establish and communicate procedures on the information security incident response to all relevant interested parties. These incidents are to be responded to by a designated team with the required competency. The response is to include a minimum of: • containment (of a security event and limit its impact to the organisation, customers and their information) • collecting evidence as soon as possible after the occurrence • escalation (as required), including crisis management activities and possibly invoking business continuity plans (BCPs) • ensuring that all response activities are properly logged for later analysis • communicating the existence of the information security incident or any relevant details to relevant internal and external interested parties (following the need-to-know principle) • coordinating with internal and external parties (i.e., authorities, external interest groups and forums, suppliers, and clients) to improve response effectiveness and help minimise consequences for other organisations • once the incident has been successfully addressed, formally closing, and recording it • conducting information security forensic analysis (as required) • performing post-incident analysis to identify root cause. Ensure it is documented and communicated according to defined procedures (i.e., post incident review) • identifying and managing information security vulnerabilities and weaknesses (including those related to controls which have caused, contributed to, or failed to prevent the incident) • timely notifications to be provided to the respective stakeholders (as required) on the status of the incident and resolution steps. **Resolution of an information security incident** While resolving information security incidents, organisations are to take necessary precautions to ensure the incident resolution does not lead to new or known vulnerabilities. Any vulnerabilities identified during incident resolution process are to be isolated, treated with caution and reported to respective professional bodies Additional activities identified as part of incident resolution are to be tracked for continuous improvement purposes.

Functional Process	Control Area	Requirement	Guidance
			Post incident report The process of reviewing and documenting the impacted areas, personnel, and processes following an incident after its resolution is known as a post incident report. The documented report consists of: • a timeline of communication and steps taken • a list of resources used in the response and their effectiveness • monitoring information to provide context for the system's health, to judge response effectiveness • comments from responders giving insights on what was helpful and what wasn't • suggestions for improvement(s) to the response process. In all instances where a situation may lead to an external investigation or legal proceedings, a qualified external resource is to be engaged to carry out the investigation. This might result in removing the device from the infrastructure which may pause the affected applications or services. In such scenarios, documented incident management plans are to be used.
Identify	Roles and responsibilities	HML23: Organisations are to have roles and responsibilities determined to carry out the incident management process.	**Roles and responsibilities** Roles and responsibilities for carrying out incident management procedures are to be determined and effectively communicated to the relevant internal and external interested parties. At a minimum, consider: • establish a common method for reporting information security events, including point of contact (i.e., service desk contact number, tool, or email ID) • an incident management process, providing the organisation with capability for managing information security incidents including administration, documentation, detection, triage, prioritisation, analysis, communication and coordinating interested parties • an incident response process, providing the organisation with capability for assessing, responding to, and learning from incidents • only allowing competent personnel to handle the issues related to information security incidents within the organisation. Such personnel are to be provided with procedure documentation and periodic training • a process to identify required training, certification, and ongoing professional development for the incident response team • ensuring communication, to both internal and external parties, is shared via authorised channels only. It is recommended to have a RASCI (Responsible, Accountable, Supporting, Consulted, Informed) matrix readily available and documented for effective incident management, identifying what roles are to be performed by internal teams and suppliers.
Respond	Collection of evidence	HML74: Evidence gathered as part of the incident management process is appropriately protected.	**Collection and protection of evidence** Organisations will need to consider the implications of collecting evidence for purposes of investigating all identified information security incidents. Internal procedures are to be developed and followed when dealing with evidence for the purposes of disciplinary and legal actions. In general, these procedures for the management of evidence are to provide instructions for the identification, collection, acquisition, and preservation of evidence in accordance with different types of storage media, devices, and status of devices (i.e., powered on or off). Organisations are to seek advice on their next steps from Te Whatu Ora, NCSC, CERT NZ, Office of the Privacy Commissioner (as applicable) during the time of the incident. There is often a trade-off between collecting evidence and addressing incident threats propagating throughout a network. Evidence typically needs to be

Functional Process	Control Area	Requirement	Guidance
			collected in a manner that is admissible in the appropriate national courts of law or another disciplinary forum. It is possible to show that: • records are not complete and have been tampered with • copies of electronic evidence are not identical to the originals • any information system from which evidence has been gathered was not operating correctly at the time the evidence was recorded. Where digital evidence surpasses organisation or jurisdictional boundaries, the organisation is to ensure it is entitled to collect the required information as digital evidence. When an information security event is first detected, it is not always obvious whether the event will result in court action. Therefore, the danger exists that necessary evidence is destroyed intentionally or accidentally before the seriousness of the incident is realised. It is advisable to involve legal advice or law enforcement early in any contemplated legal action and take advice on the evidence required.
Respond	Learning from an information security incident	HML75: Organisations report all security incidents and near misses to the organisation's senior management or to the Board by a nominated Information Security Officer.	**Lessons learned from information security incidents** As part of a continuous improvement process, the organisation's senior management and the Board or applicable steering committee is to be notified on all information security incidents (including details of high priority incidents). Higher priority incidents are to be monitored following resolution to ensure new vulnerabilities are not introduced. A standard monthly report on all security incidents is to be provided to the organisation's senior management or governance body. The incident reports, at a minimum, are to include: • the nature of the security incident or near miss • action taken • actual/potential impact on information security/business continuity • remedial action taken • any countermeasures/changes to information security settings to mitigate risk(s). Any new risks identified as part of the incident resolution are to be documented within the organisation's risk register. The knowledge gained from information security incidents, and testing of plans, is used to strengthen and improve the information security controls, including: • enhancing the incident management plan, including incident scenarios, and any associated assets or procedures • identifying incidents (both one off and recurring) with major impact(s) and their causes, to support updating the organisation's information security risk assessment, risk register and implementing any necessary additional controls to reduce the likelihood or consequences of future similar incidents. Mechanisms to support this can include collecting, quantifying, and monitoring information about incident types, volumes, and costs • enhancing user awareness and training by providing examples of what can happen, how to respond to such incidents, and how to avoid them in the future. Additionally, the summary of the incidents is also reported at the Board or steering committee meetings at which the minutes are documented. These meeting minutes are referred as evidence at the time of audits. High priority incidents are to be reported to Te Whatu Ora and, as applicable, to NCSC, CERT NZ and the Office of the Privacy Commissioner within 24 hours of detection.

Functional Process	Control Area	Requirement	Guidance
Business continuity and disaster recovery management Implementation of controls in this section ensures: • information and associated assets are protected during disruption • information and applicable operations are restored at the required level and in the required timeframes.			
Plan	Information security during disruption	HML08: Documented, approved, business continuity and disaster recovery management, operational resilience policies and procedures are established.	**Business continuity and disaster recovery plans (BCPs & DRPs)** For adapting information security controls during disruption, the organisation's information security requirements are to be identified as part of business continuity management plans. To restore or maintain the security of information and critical business processes, the developed plans are to be tested, reviewed, approved, and evaluated periodically so that they are up to date. These plans also outline the importance of maintaining the security of information, the services that are being provided at an appropriate level during disruption. While developing, implementing, maintaining, and reviewing the business continuity and disaster recovery plans, organisations, are to consider: • identifying the processes, systems, information, and other relevant equipment critical to patient care • that plans are appropriate to the organisation's information security and business objectives • that the objectives for business continuity and disaster recovery contains a framework • the risk appetite of the organisation including the maximum tolerable time the organisation cannot provide its services (recovery time objective – RTO) and the maximum amount of information an organisation is willing to lose during a disruption (recovery point objective – RPO) • information security controls, supporting systems and tools (as necessary) and the processes to maintain them during disruption • the compensating controls for information security which cannot be maintained during disruption (including physical and environmental factors/threats such as fires, medical emergencies, tornadoes, hurricanes, flooding, earthquakes, and other natural disasters) and civil disruptions (e.g., strikes, outbreaks) • the plans, including the roles and responsibilities, are being supported by regular workforce training along with defined lines of communications • fall back procedures and dependencies (as necessary) to counter failure in documented processes, existing systems and relevant equipment that are critical in healthcare delivery • maintaining contact details of relevant suppliers and emergency authorities (including first responders and other law enforcement entities). **Information security requirements** To maintain information security requirements in the event of a disruption or a failure, usually, a business impact assessment (BIA), and risk assessment are performed for the identified critical services and systems. This helps the organisation understand the potential consequences of a loss of information (either of confidentiality or integrity, and to prioritise the need for maintaining availability) of the critical systems and services their business operations along with the services that are being provided to their customers. Business continuity and disaster recovery plans are to be tested and reviewed periodically (at least annually or when there are significant changes affecting patient care/technology) so that they are current, available and

Functional Process	Control Area	Requirement	Guidance
			accessible to personnel as needed. As patient lives can depend on access to patient data, it is important for organisations to include health crisis management planning as a critical consideration. While managing business continuity, where ICT continuity plays a key part, consider the following requirements to maintain minimal disruption to the availability of information: • regardless of the event, how will the organisation respond and recover from the disruption to services • prioritised services or activities are supported by the required technology • detect and respond to the alerts raised while monitoring activities which could result in disruption or failure of services to patient care. It is recommended to have designated communication channels established in the event of disruption or failure, to allow for clear and effective communication with both internal and external interested parties. This helps to communicate information to participants and stakeholders, assess and relay damage, and coordinate a recovery strategy.
Identify	ICT readiness for business continuity	HML24: Establish criteria for developing business continuity, disaster recovery, operational resilience strategies, and capabilities are to be determined based on disruption and impact to the organisation.	**Business impact analysis (BIA)** A BIA is performed to determine the IT readiness, security requirements that are to be maintained in the event of failure or disruption. As part of the BIA, the impact types and the criteria to assess the impact over a period of time are to be considered to estimate any disruption caused in providing patient care. Based on the type of impact, the services required to provide patient care are to be identified, prioritised and an RTO is to be assigned (along with resources including IT services, and documented disaster recovery procedures). The BIA is expanded to define performance and capacity requirements of ICT systems, and RPO for information and services required to support patient care during disruption. When performing a BIA, at a minimum, consider: • critical services, processes and systems along with their dependencies (i.e., information, applications, systems, networks, workloads, etc), with identified inherent risks • the likelihood and impact of each inherent risk materialising, causing loss or degradation of critical services and systems • the risk appetite and tolerance of the organisation i.e., the impact or damage the organisation can tolerate • risk dependencies • the identification of appropriate and relevant countermeasures or complementary controls, to prevent and detect the identified risks • the immediate and ongoing impacts, resulting from disruptions • RTO and RPO • the estimated internal and external resources required for recovery and resumption. Once a BIA is performed, the results are used to document the continuity plans, along with: • business, ICT continuity requirements and objectives include performance and capacity specifications • RTO and RPO for all prioritised services for restoration • RPO of the prioritised IT resources (defined as information required for patient care and the procedures for its restoration).

Functional Process	Control Area	Requirement	Guidance
			The business continuity strategies are identified and selected by the organisation before, during and after disruption, based on the outputs from the risk assessments and BIA performed. Respective plans are to be developed, tested, and maintained to meet RTO and RPO requirements as defined in the BIA. The identified strategies and plans are to: • be developed by considering inhouse and cloud services which are being used to provide business critical services • consider the impacts and risks identified before, during and after disruption or in the event of failure • consider and cover all actions within the required timeframe, by aligning with the organisation's risk appetite for prioritised services by reducing the likelihood of disruption • include detailed plans and procedures for implementation • ensure the competency of assigned personnel and sufficient service capability along with workable plans designed to ensure the agreed service continuity levels are maintained following major service failure or disaster • ensure the availability of an alternative facility (i.e., disaster recovery site). In addition to the above, documentation supporting the identified critical services, solutions, and solution procedure(s) is to be made available and reviewed periodically to reflect the organisation's current environment. The documentation supporting the continuity of information and services is to include: • solution architecture diagrams • administrator and user guides • backup and restoration procedures • software bill of materials (SBOM) (inventory of all components and software dependencies) • configuration guides (where applicable) • documented business continuity plans or fall-back procedures with a BIA and escalation procedures.
Protect	Information security during disruption	HML35: In the event of a disruption or failure, critical information or services are identified, and measures are taken for the continuity of services.	**Maintaining availability** To maintain the availability of critical services and systems containing information, the organisation's requirements are identified for its redundancy and implemented at an architecture level. The architecture documentation (which is created and maintained) helps with understanding if the services and systems are to be manually or automatically activated (as and when required). Organisations are encouraged to configure alerts so that they are notified in case any of the services and systems could potentially be unavailable (so that continuity plans can be implemented as required to maintain the availability of information). While implementing redundant systems, consider: • internet service provider, power supply – contracting with a minimum of two suppliers that do not share the same internet backbone • data centres – the services are mirrored between data centres which are geographically separated and are not with the similar threat landscape • hardware – have duplicated systems with configurations and network connections • cloud services - have duplicated data and systems in different geographic locations • information – offline, backed up information is tested periodically for restoration purposes and the results documented to ensure data can be restored successfully within agreed timeframes.

Functional Process	Control Area	Requirement	Guidance
			Implementation of redundancies possibly will introduce risks to maintaining integrity of information, along with confidentiality requirements. These risks are to be considered during the architecture phase. In case of cloud services, it is recommended to plan for an automatic failover and load balancing between multiple physical locations which are geographically segregated. If any of these services are outsourced to a supplier, contractual arrangements, or service level agreements (SLAs) are to be documented to maintain and monitor the redundancy to the systems and services.
Detect	ICT readiness for business continuity	HML63: The lessons learned from business continuity and disaster recovery testing are reflected in the established and implemented information security controls.	**ICT readiness** After an emergency or disruption to an organisation, its readiness to maintain the critical functions is known as business continuity and the method of regaining its access to its IT infrastructure is known as disaster recovery. Business continuity and disaster recovery plans are usually developed and tested for use in case of disruptions, to maintain availability of information, and to provide continuous patient care. The documented BCP and DRP are to be tested annually at a minimum, or as and when there are significant changes being made within the organisation. While performing these tests or reviews, consider: • failover and failback testing • processes documented within the business continuity plan • alignment with the RPOs and RTOs (as defined during a BIA) • roles and responsibilities of the various parties involved in the exercise • review and updating (as required) of communication templates • lessons learned from previous events and exercises • tabletop exercises to help simulate potential events and test the response lifecycle of all involved parties. There can also be a disaster recovery plan, which is usually part of tabletop exercises, involving local authorities like the fire department, health officials, police department, Office of the Privacy Commissioner, etc. These exercises or tests are usually performed on non-production environment(s) so that patient care is not affected. It is important to note that the business continuity plans are different from disaster recovery plans. A failover or failback disaster recovery (DR) exercise is to be conducted annually for critical services and systems. Organisations are to remain cognisant of the role that information systems play in patient continuity of care and are to be prepared for if/when IT systems fail.

Functional Process	Control Area	Requirement	Guidance
Supplier management Implementation of controls in this section ensures: • information and associated assets accessed, managed, or provided by suppliers are protected • an agreed level of information security and service delivery in supplier relationships is maintained.			
Plan	Policy for suppliers	HML09: The information security requirements for managing the risks while a supplier is accessing information are to be identified and communicated.	**Documented policy or procedures** A Supplier Management Policy or procedure on the supplier relationships lifecycle is to be documented, approved, and shared with authorised personnel. This document helps organisations to optimise their procurement efforts and improve their performance. An effective supplier management policy or procedure establishes a good working relationship with the suppliers by setting expectations early on, and clearly communicating what is to be expected. **Supplier selection** When a supplier is being selected, a documented procurement process is to be followed along with consideration of business and security requirements. Organisations are to review available third-party assurance reports (i.e., ISO 27001, SOC 2 Type II, etc) for systems and services which are being provided by the supplier. In addition, organisations are to identify the associated risks if any information is potentially accessed by the supplier to manage the systems and services which are being provided. Security controls are selected and agreed with the supplier where applicable, to manage identified risks. Performing a risk assessment is effective for managing the supplier's access to information. Processes and procedures are to be identified for managing the risks which are not at an acceptable level (as per the organisation's risk management framework) and are to be reviewed periodically. It is recommended that, at a minimum, all critical risks are reviewed every 4-6 weeks, while medium to high risks are reviewed every quarter. **Inventory** Maintaining an inventory of suppliers (including cloud services) to manage supplier agreements within the organisation by relevant personnel is recommended. This inventory is to contain a minimum of the following, and be reviewed periodically to note any changes in services which are being provided by the suppliers: • supplier name • cloud or on-premise • services which are being provided • classification of information which is being hosted • ownership of information along with intellectual property • contract expiry • contract or agreement renewal date • contact information (internal) • contact information (supplier) • security assurance activities performed • documents reviewed as part of assurance activities • any concerns identified • risk assessment performed

Functional Process	Control Area	Requirement	Guidance
			• BIA documented along with RPO, RTO • escalation contact points • subcontractors or supply chain details • key contacts for incidents • jurisdictional limit to which NZ information is to be shared for processing, use or storage • legal, regulatory and compliance requirements maintained by the supplier • previous and next review/audit date for the supplier. **Maintaining a supplier relationship** While drafting the document and working with the suppliers, consider: • engaging suppliers with a focus on building trust, co-operative and long-term relationships • working collaboratively to better anticipate changes to risk profiles and the threat landscape • periodic review of the contracts such that they suit contract management • performance management by obtaining regular service reports • continuous improvement of existing services through service optimisation • development of a responsibility assignment matrix for supplier management. This sets out who is Responsible, Accountable, Supporting, Consulted and Informed in each activity, with respective cyber security teams supporting supplier management and being informed of any changes in suppliers. **Notification of legal investigations** Organisations are to be notified of any legal investigations (including e-discovery by their supplier located in other countries on a multi-tenancy environment) occurring with their supplier(s), so that they are aware of what information is being made available to other 3rd party organisations. Additionally, their supplier(s) may have headquarters overseas and information may be shared across jurisdictions. This notification requirement is typically documented within a Master Service Agreement (MSA) between the organisation and their supplier.

Identify	Supply chain risks	HML25: Suppliers are to be systematically evaluated, and their information security activities are reviewed before and after onboarding of their systems and services.	**Risk assessment activities**
			Cyber security is to be considered as a fundamental element of supplier selection, in the same way as pricing or delivery timeframes while procuring new services or applications (or when changes are being made to the existing ones). While selecting suppliers, a cyber security risk assessment is to be performed to determine the risks the organisation while using a supplier's service. When selecting suppliers and performing risk assessments, consider:
			• the level of access the supplier has to the organisation's systems and the frequency of that access
			• the access the supplier has to the organisation's intellectual property, information, or other sensitive data
			• whether the supplier could likely be used by a third party as a vector to attack or disrupt the organisation or patient's care
			• the organisation's level of financial dependency on the supplier
			• the impact to the organisation and patients if the supplier experienced a major disruption
			• the time and cost in restoring or maintaining the organisation services if there was a sudden loss of access to the supplier's products or services
			• areas which might need improvement to protect organisational information to include:
			  • information security standards, controls and procedures
			  • malware protection and threat management systems

Functional Process	Control Area	Requirement	Guidance
			• identity and access management procedures • audit and compliance procedures • documentation standards • data access controls • data lifecycle management • physical security procedures • incident management procedures • quality assurance procedures • distribution channel security • commitment to security assurance throughout a product or service's lifecycle • jurisdiction where information resides at • sub-contractors (if any) • zero trust architectural design considerations. Based on the results of the risk assessments, use of additional security controls both internally and at the supplier level to maintain confidentiality, integrity and availability of the information are to be considered. Strong, collaborative security relationships with supplier(s) is to be developed to improve the flow of information and assist with co-ordination, especially during a security incident. It is important to listen to suppliers' feedback, seek to address concerns they may have about the organisation's security arrangements, and endeavour to provide support or information they require, where possible. **Continuous availability** A BIA is to be performed to identify the organisation's critical assets, products and services, to monitor supply chain risks. The BIA is described in detail under the Business Continuity and Disaster Recovery Management domain. These risks might result in additional threat actors due to the organisation's weakness in maintaining security of information systems, where examples include: • inserting malware into the organisation's services or systems via compromised software or code provided by a third party • a compromised supplier, giving an attacker unauthorised access to the organisation's systems and data using the supplier environment as the attack vector • an insider personnel is employed by a supplier who uses the organisation's systems to conduct malicious activity • counterfeit or compromised hardware components are inserted into the supply chain • poor quality-control in a software development or production process is exploited by a malicious actor • systemic vulnerabilities are discovered • virtual infrastructure is disrupted (for example during a DDoS attack) • tenant segregation failure, resulting in information disclosure to unauthorised parties • cloud service provider being locked-in resulting in loss of information availability when moving to a different cloud service provider • service provider fails to delete information after the organisation no longer retains their services, resulting in information disclosure

Functional Process	Control Area	Requirement	Guidance
			• data migration failure, resulting in information loss.
Protect	Information security within supplier agreements	HML36: The organisation's information security requirements are to be included in the agreements with the suppliers.	**Agreements with suppliers** Agreements or contracts with suppliers are important to establish the delivery of a set of products or services and provide a record of commitment. They also serve as a collaboration and communication tool with the terms specified within, while increasing operational efficiency. Once the supplier is selected, the agreements are to be clear such that the supplier understands their obligations, along with the organisation's information security requirements. While documenting the agreements, consider: • a clear description of the information, the privilege which can be granted and how it can be accessed • legal, statutory, regulatory, and contractual requirements on data protection and handling patient and personal information • what and how intellectual property rights and copyrights to the information are protected • obligations to implement additional security controls or improve existing controls (as required) to protect information, including backup of information or other mechanisms to maintain its availability • service reports on the performance review of the services, monitoring, and the right to audit security controls or providing independent third-party assurance reports (such as ISO 27001, SOC 2 Type II, PCI DSS, etc.) • security review (certification & accreditation activities, penetration testing and vulnerability assessment reports as applicable) of a supplier undergoing change of ownership, change of major shareholding, or a merger • suppliers' obligation to comply with the organisation's information security requirements • performance reports on the services which are being provided • acceptable use of information and organisation assets during the term of the service and after termination of the contract • personnel screening requirements (e.g., Ministry of Justice checks, qualification checks), onboarding and offboarding processes of supplier's staff • clauses or compensations for breach of contract or failure to meet contract requirements • vulnerabilities disclosed by the public need to be effectively communicated to the organisation and managed by the supplier • collaboration in managing incidents, • updates to the services which are being provided within agreed timeframes • incident or problem resolution and conflict resolution processes • change management process (including managing patches and known vulnerabilities) are being followed for the affected information and services which are being affected to maintain compatibility of the existing technologies • communication to organisations when vulnerabilities are identified and how they are contained • approved secure mechanisms for sharing or transferring information either physically (e.g., papers) or logically (e.g., file transfers) • additional training requirements for organisation's staff as and where required and maintaining up-to-date documentation • processes or obligations for having sub-contractors provide the services (as per the agreement) • contact information and escalation points in case of incidents • considerations about legal jurisdictions and data sovereignty depending on where the information is residing

Functional Process	Control Area	Requirement	Guidance
			• termination and exit clauses including information management, return of assets, secure disposal of information and associated assets, confidentiality obligations, and handover to the organisation or another supplier. It is the organisation's responsibility to regularly review, validate and update their agreements with their supplier(s) to confirm that they are valid and fit for purpose. **Reporting metrics** Key reporting metrics are to be established, along with regular validation of the services being provided by the supplier, in the form of service reports. These service reports are usually used as input to the organisation's cyber security programme, to manage potential risks. When receiving reports from suppliers, consider (as applicable and based on the signed agreement) the minimum of the following to be reported on: • incident response times • RTO and RPO for services that are being managed • patching cycles and maintenance schedules where regular validation is to be defined using an agreed schedule and based on the criticality of the services which the supplier provides • capacity management reports (as applicable) • regular testing including penetration and vulnerability assessment reports • results of backup, restoration and testing procedures • results of internal or external audits • incident or problem resolution and conflict resolution processes • changes to suppliers' internal processes affecting the organisation.

Functional Process	Control Area	Requirement	Guidance
Cryptography Implementation of controls in this section ensures that confidentiality and integrity of information is maintained while in transit and at rest.			
Protect	Use of cryptography	HML37: Rules for effective use of cryptography including encryption and key management are defined and implemented.	**Cryptography** Implementation of cryptographic mechanisms ensures that information is not altered during transit between the sender and the recipient and while in storage. Information is to be secured during its transmission as per legal, regulatory, and contractual requirements to protect from malicious third parties. This could be achieved by using encryption algorithms (such as TLS) that protect communications that traverse untrusted networks, to avoid data and identity theft cases by protecting: • confidentiality of information: encryption is used to protect information when it is either being stored or transmitted. • integrity or authenticity of information: message authentication codes (MACs) or digital signatures could be used to verify the authenticity or integrity of information that is stored or transmitted. Algorithms could be used to check file integrity issues. • non-repudiation: used to provide evidence of who or what performed a particular action. • authentication to access information: ensures a person or entity is who they claim to be before they have access to information. When using encryption mechanisms, it is important for organisations to ensure that the potential risk of disclosure of the information is reduced, and consider: • defining cryptography or encryption procedures (or guidelines) to protect information, and the risk of not using cryptographic techniques (including inappropriate or incorrect use) is minimised • the required level of protection for information (if it is held on mobile user endpoint devices, storage media or transmitted over networks) is identified • how encryption keys (including the ways to generate and protect their encryption) are managed, along with information recovery (if the keys are compromised or lost or damaged) • organisation roles and responsibilities for effective use of encryption, and key management (including minimum baseline requirements or protocols which are approved for use) • the way the encrypted keys are stored (i.e., not stored in plain text and made available to authorised personnel only) • validation of digital signatures, e-seals and certificates. The requirements for liability, and response times are to be covered within service level agreements or contracts with external suppliers for encryption services (e.g., with a certification authority), including use of symmetric keys (for data-at-rest) or asymmetric keys. **Key management plan** Information is encrypted and decrypted with the use of encryption keys, meaning any loss or compromise of any encryption keys would invalidate the data security measures which are in place. To support the management of encryption keys, there is to be a key management plan by considering:

Functional Process	Control Area	Requirement	Guidance
			• description of the system or service (including the environment), the cryptographic system topology (including data flows), use and ownership of keys, key algorithm, key length, and key lifetime • roles and administrative responsibilities (whether the keys are managed in-house via a hardware security module (HSM) or outsourced or automatically updated by systems administrator), including the responsibilities of a record keeper and how an authorised user obtains access • administrative tasks which are to securely generate, exchange, store, rotate, temporarily or permanently suspended, lost, corrupted, revoked, expired, compromised, or destroyed encryption keys (along with their backup and archival procedures) • information security incident playbooks where the keys could be compromised • key generation and setup for different encryption mechanisms as suitable for relevant applications or services or systems (e.g., setting up private keys, generating SSH private/public keys, SSL/TLS certificate generation or rollouts, etc) • issuing and obtaining public key certificates • logging and auditing of activities relating to key management • configuring activation and deactivation time periods for keys (so that keys are used only for the period of time as documented in the organisation's policy or procedures) • encryption keys are protected against modification and loss (where secret and private keys are protected against unauthorised use and disclosure) • legal, regulatory, and contractual requirements are met • protection and maintenance of software and hardware (including destroying encryption keys as required) • mitigation strategies to accommodate the risks if keys are owned by the organisation or the supplier, or if they were to be distributed to intended parties including how they are to be activated. **Key lifecycle & authentication** Procedures are to be documented on the lifecycle (create, maintain, terminate/expire) of encryption keys for relevant applications, services or systems. Unique lifecycle for credential rotation of critical systems is to be documented along with the frequency of the rotation. If there is a potential incident, the keys are to be terminated, and new keys are generated to maintain the security of information. Logs of accessing these keys are to be recorded and monitored to identify any unauthorised access (including details of roles and personnel with system administrator access along with personnel whose access was disabled or withdrawn). In addition to the above, the authenticity of the public keys needs to be addressed by the certificate authority who issues public key certificates.

Functional Process	Control Area	Requirement	Guidance
Identity and access management Implementation of controls in this section ensures: • individuals and systems accessing the organisation's information and devices are to be uniquely identified • individuals and systems are to be authenticated, and circumvention of the authentication process is prevented • access to information and associated devices is to be defined and authorised according to the business and security requirements.			
Plan	Access control	HML10: Establish, document, approve, and implement rules to control physical and logical access to information and its assets.	Organisations with information and devices are to have only authenticated and authorised personnel to access the information and its associated assets. These owners are responsible for determining the business and security requirements of the related information assets, including the personnel who have access to them (and the duration for which access is granted). **Identity and access management policy or procedure** An identity and access management policy or procedure is to be implemented, considering business and security requirements to prevent unauthorised access to information and its associated assets. This policy or procedure is to be formally documented, approved, published, communicated to relevant parties, and reviewed regularly. While documenting, consider: • which roles require what level of access and permissions (i.e., authorisation level) to information and its associated assets (i.e., the need-to-know principle) • business and security requirements (i.e., need-to-use) • a risk-based approach to securing the authentication information of the user (i.e., multi-factor authentication (MFA)) based on the type of network, device (e.g., organisational asset or BYOD) and systems being accessed. For unmanaged devices (BYOD), the lifetime of each authentication session could be reduced to shorten the length of time a given token is viable • security of relevant applications • appropriate security controls to protect the assets • restrictions to privileged access • segregation and rotation of duties requirements (where and when applicable) • relevant legislation, regulations, and any contractual obligations regarding limitation of access to information, associated services and assets • process of authorising access requests • management of access rights • creation and management of system accounts • logging and monitoring • configuring system alerts for abnormal activities with registered accounts • regular access reviews for all account types • principle of least privilege • physical access to information assets. Procedures to provide access for critical services are to be used only in emergency situations and based on the security principle of just-in-time access where approval(s) for access provisioning is to be documented for reference purposes.

Functional Process	Control Area	Requirement	Guidance

Protect	Identity management	HML38: The complete lifecycle of the account(s) being used to access, process, or manage information and services is managed.	**Unique identity**
			Organisation's processing, storing, or managing information and devices are to have a unique identity for individuals to access systems or services, ensuring that appropriate access is provided and maintained. There shall be a formal user access creation process, enabling a unique identity which is consistent with the access permissions needed. There is possibility for a variety of accounts within the organisation, such as:
			• standard user account:
			a day-to-day account used by personnel. These accounts are provided to individual users in order for them to access information on the organisation's network and are linked to a single person.
			• privileged access:
			permissions that enable one or more of the following:
			  • the ability to change control parameters
			  • the ability to change key system configurations
			  • access to audit and security monitoring information
			  • the ability to circumvent security measures
			  • access to all data, files and accounts used by other system users, including backups and media
			  • special access for troubleshooting the system.
			• privileged account:
			an account that is used almost exclusively to perform actions based on privileged access. In almost all cases, a privileged user account will be issued to individuals with a standard user account (which is used for day-to-day purposes).
			• service account:
			a special type of non-human privileged account, used to execute applications and run automated services, virtual machine instances, and other processes.
			• supplier account:
			an account used by a supplier to access the systems and devices on the organisation's network.
			• just-in-time account:
			an account type that is provisioned in the privileged access management system that allows administrators to perform tasks if their privileged access accounts are not available to perform these tasks. It is usually provisioned for a specific duration until the task is over.
			• break glass or emergency account:
			an account that allows access when other privileged accounts do not authenticate. This account bypasses normal controls and so its credentials are stored offline. Note: break glass does not refer to a medical procedure.
			
			All user accounts are to be provided access to systems containing information as per documented business and security requirements:
			• upon verifying that the individual is an authorised system user (i.e., after relevant background checks including relevant qualifications are completed)
			• are named accounts (i.e., all accounts are to have a structurally approved naming scheme that is consistent with the users' identification e.g., firstname.lastname).
			
			If there is no business use for any type of account, or if the user leaves their organisation or supplier organisation, it is recommended to disable access within appropriate time periods, with reviews performed periodically to note that the right access is being provided to the users.

Functional Process	Control Area	Requirement	Guidance
			For supplier managed systems or services, a zero-trust architecture with the supplier is to be maintained along with documenting any associated risks which are known and appropriately treated. **Access creation and modification** For user access creations and modifications, organisations are to ensure that the request is authorised by the requestor's manager and approved by the system or business owner (i.e., to confirm the business requirement) before access is granted. Separate approval processes from management could also be appropriate. In case of temporary access, it is strongly recommended that the access is restricted to a limited time-period (i.e., just-in-time access). User accounts are to be disabled when there is no business and security requirements for an individual or a service account to have access to information and associated systems. To remove unnecessary or outdated permissions, regular access reviews are to be performed to prevent unauthorised access on all types of accounts and their associated assets. User accounts are to be disabled when there are no business and security requirements for an individual to have continuing access to information and associated assets. In the health sector, it is important to note that although patients are not users of any systems, they have access to their information via online portals for which access reviews cannot be performed.
Protect	Information authentication	HML39: User accounts are authenticated and circumventing the authentication process is prevented.	Organisations processing, storing, or managing information and its associated assets are to ensure that their information systems, services, and network resources are protected, by permitting only authenticated users or processes to gain access to their protected resources. Authentication helps to prove that an individual or service accounts are who they or the service claims to be. **Authentication** Authentication is the process of verifying that you have the right to access an account either via username and password, or PIN, or access cards, or physical tokens, or biometrics. While allocating authentication information, organisations are to ensure that: • passwords or PINs generated during enrolment are changed after first log-on • default username and passwords provided by the supplier or manufacturer are to be modified, especially for administrative accounts • documented processes are available for new or temporary authentication information and the information is shared in a secure manner • if the authentication information cannot be changed, the information is kept securely to maintain its confidentiality. Organisations are to protect the authenticated information and process throughout all stages of the information lifecycle. **Authentication mechanisms** Strong authentication mechanisms could be used for checking a user's identity when passwords or PINs are not sufficient (e.g., administrative accounts, privileged accounts). This usually combines two or more different authentication factors below to improve the security of information system: • what you know (e.g., username or password)

Functional Process	Control Area	Requirement	Guidance
			• what you have (e.g., device or security key) • what you are (e.g., fingerprint or your face) • where you are (e.g., geolocation or IP based) • which device or operating system is being used (e.g., only organisation issued devices are to be granted access). It also includes the zero-trust principle which is to be applied where possible (where people, devices and networks are authenticated and authorised individually, regardless of whether they are accessed internally or from outside the network perimeter). In organisations, when providing patient care in emergency situations, the time pressures involved could make the use of passwords difficult, during which alternative authentication mechanisms (such as biometrics) are to be used to protect information and devices from unauthorised access. It is also the responsibility of the personnel who are accessing information that: • passwords and PINs are allocated as per documented procedures and kept secure • if there is an indication or notification that the authentication information is compromised, it is to be changed immediately • it is recommended to enforce an organisation's approved password policy, with exceptions documented along with their business requirements. Passwords are used in many authentication scenarios and have a limited ability to protect information and devices. It is recommended to use passwords only when they are required. Otherwise, authentication mechanisms such as single sign-on (SSO) is recommended at an organisational level, along with multi-factor authentication (MFA) for user accounts with heightened privileges and internet facing systems and services. Organisations are to ensure that a robust password policy enforces secure authentication mechanisms. When passwords and PINs are used as authentication methods, consider that: • passwords are managed and comply with the organisation's password policy • allocated passwords are changed at first log on • not to be used in more than one system, or used on personal accounts • passwords are not used in more than one system (or used in personal accounts) • passwords are not to be reused over time (based on password history requirements) • passwords are forced to be changed if there is a possibility that it has been compromised (or when a staff member leaves, and they have access to a shared account) • passwords are not shared with others • passwords are not displayed in clear text when being entered • approved password manager is used to save passwords. Applications or services where passwords cannot be changed after first log-on are to be identified and associated risks are to be documented and managed, with compensating controls being implemented. For service and emergency accounts, passwords are to be stored and shared in a protected form (e.g., password manager). For break glass accounts, passwords are to be stored offline in a tamper evident envelope in a locked

Functional Process	Control Area	Requirement	Guidance
			drawer with a secure PIN. Access to these drawers is to follow an approval process from senior management. In all these scenarios, passwords are shared with authorised personnel only, based on their roles and responsibilities and in line with business and security requirements. Any required changes to the break glass accounts are to follow rigid approval processes before they are implemented. **Preventing authentication** Occasionally it is necessary to prevent users or accounts authenticating access to a system or the network (e.g., lost authenticators may be retrieved by an unauthorised person or blocking access to personnel known to demonstrate malicious activity). Accounts can be prevented from authenticating through several mechanisms: • revocation or replacement of keys or authentication information • disabling or removing the account.

Protect	Access rights	HML40: Access to information and its associated assets is defined and authorised according to the business and security requirements and adhere to the organisation's identity and access management policy or procedures.	**Provision of access**
			The services and applications used by organisations to support continuous patient care through the use of information and devices, is to only be accessed by personnel based on their roles and responsibilities. The creation, modification and deletion of these access rights is to follow a documented and approved process, which is to be periodically reviewed to reduce the likelihood of unauthorised access to information and is to be provided using the principle of least privilege. While documenting this process, consider for both physical and logical accesses:
			• access creation, modification, and deletion:
			  • personnel are trained prior to being given access to system(s)
			  • a request is raised via a formal channel
			  • the raised request is authorised by requestor's manager, or custodian of information or device owner, considering business, security, and privacy requirements. Access is activated only after the request is approved by the business or system owner
			  • segregation of duties (for approval, implementation, along with separation of conflicting roles)
			  • the level of access provided is in accordance with the documented policy or procedure
			  • access is activated only after relevant checks are performed, or required clearances are obtained
			  • access rights are modified or adjusted for personnel who have changed roles within the organisation
			  • access provided is removed when someone no longer needs access to information and assets, especially when they exit from the organisation
			  • temporary access is provided for a limited time period with relevant approvals, and removed on the date of expiration (unless otherwise extended especially for locums, interns, volunteers, etc)
			  • maintain a central record of access rights granted to information and its associated assets (ID, logical or physical).
			
			It is strongly recommended to consider terminating the access rights within the organisation as and when there is a notice of removal, termination or resignation where there could be an increased risk if information is accessed.

Functional Process	Control Area	Requirement	Guidance
			Access reviews Access reviews are to be performed: • periodically at a minimum of every quarter for personnel with regular access rights and more frequently (i.e., at a minimum of every month) for access rights with heightened permissions • as and when there is any change with personnel's role within the same organisation (e.g., job change, promotion, demotion, decommissioning a supplier) or resignation, or termination of employment.
Protect	Privileged access rights	HML41: Organisations are to ensure that only authorised users, software components and services are provided with privileged access rights.	**Elevated or heightened permissions** Special permissions are required to allow organisations to secure information, devices, systems, and applications while maintaining confidentiality and to protect from unauthorised access. The management of privileged access rights supports the principle of least privilege and just-in-time access as it provides an oversight to manage or mitigate the risk of accounts that have capabilities beyond the standard user. Only authorised personnel and services are to be given heightened permissions or privileged access, and this authorisation process follows the organisation's identity and access management policy or procedures. While providing privileged access rights, consider: • personnel are trained before they are given access to system(s) • access is provided only after the requests are authorised, once business and security requirements are verified • privileged accounts are to be linked by common identifiers so that there is a clear segregation of actions • unique accounts are to be assigned • privileged accounts are not shared between personnel • additional authentication mechanisms (e.g., MFA) requirements enforced at the organisation's policy level • provided with just-in-time (JIT) access where access is limited to predetermined periods of time or on an as-needed basis • access to web applications including webmail and web access is to be restricted • not be used for standard user activities i.e., not designed for day-to-day computing and has access to perform tasks like installing applications, editing registry or anything that requires elevated rights • have all their activities logged and stored for audit and security purposes e.g., users added to one of the privileged access groups, etc • reviewed at least every month or after any changes within the organisation that impact roles and responsibilities. In a few scenarios, especially while accessing patient information, it is important to note that some patient's details are restricted to a legitimate practitioner (e.g., family physician) who can share the details with a specialist. So, the applications and services supporting information are to allow health care professionals to share such information as required.

Functional Process	Control Area	Requirement	Guidance
Protect	Access to source code	HML42: Access to source code, development tools, and software libraries are restricted, appropriately managed, and maintained.	Only authorised personnel are to have access to source code for internally developed or modified applications or services. Additional controls are also implemented to prevent unintentional or malicious changes being made, while maintaining the confidentiality, integrity and availability of information. **Source code management** A source code management system is used to control the read, write and execute permissions, and access is assigned based on the personnel's role within the organisation. The write access to the source code is granted to authorised personnel or information custodians who have privilege access rights based on their roles and responsibilities. Read access is assigned for the personnel based on their roles (e.g., DevOps teams). When providing access to executable source codes or development tools or any program libraries, consider: • documented and approved procedures are to manage and maintain access to these repositories • providing access based on business and security requirements along with the roles and responsibilities • the organisation's documented and approved change control procedures are followed when any changes are being performed once the change requests are authorised • auditing and logging are enabled on all user activities in addition to changes to the source code and ingested to a centralised monitoring tool • write access is restricted for the use of open source or third-party code components if any are being used within the organisation network.

Functional Process	Control Area	Requirement	Guidance
Medical devices Implementation of controls in this section ensures: • the security requirements of medical devices connected to the organisation network are met • patient wellbeing isn't affected by potential cyber security events.			
Plan	Purchase or lease	HML11: Organisations are to include cyber security in procurement planning and decisions.	**Cyber security in procurement** Before purchasing any medical equipment, it is important to consider that they meet privacy and security requirements. Procuring and connecting medical equipment to organisation network without any due diligence could create information security risks. This is due to multiple technologies being involved to streamline internal processes for effective patient care. Organisations are to include respective IT and information security teams in the early stages of procuring medical devices that involve any technology to: • draft cyber security requirements for the medical devices • ensure that the cyber security requirements are part of the request for proposal (RFP) and tender documents • assess how the medical devices can be integrated with existing equipment in a secure way, including how they will be maintained, updated or accessed remotely • identify and manage cyber security incidents involving the medical devices • assess the type and the classification of information the procured devices will manage • consider support agreements / contracts for third-party maintenance once they are implemented.
Identify	Medical device scanning	HML26: Vulnerability scanning on medical devices is only performed when they are in a test environment not connected for patient care.	**Vulnerability scanning** Vulnerability scanning of medical devices is important to identify security vulnerabilities and manage the risks associated with the device where a nuanced approach is considered. However, when a scan is intended to be performed, care is to be taken for the devices that are connected / plugged in to patients and devices not permitted for scanning by the manufacturer. Permitted security tests are to be verified on the leased equipment and by the manufacturers to be in line with the agreed terms and conditions. Segmentation of production medical devices from the rest of the network, will ensure that it is clear what devices are being scanned and how they are being scanned can be controlled for patient safety. **Passive scans** Passive scans may be conducted by security personnel to detect security vulnerabilities or actions by a malicious actor. A passive scan uses network traffic created by existing devices to identify traffic patterns and endpoints. As it does not generate additional network traffic, it carries almost no risk of disrupting critical processes by interacting directly with the endpoint and could be advantageous for malicious actors. There is a risk that passive scans are not set up correctly, and instead introduce traffic that may compromise medical devices. Passive scans are best performed on medical devices when they are in the pre-production environment, or when they come out of the production environment for maintenance. It is best to learn which devices fall over when in pre-production than in the production environment.

Functional Process	Control Area	Requirement	Guidance
			Discovery scanning Discovery scanning is used to identify all the exposed services within the organisation's network within a defined IP address range or list of known hosts to identify the operating systems that are running on provider's network. They identify relevant information, including protocol and port usage, deployed software, misconfigured DNS servers, and unique site fingerprints on web applications. Active scans are not to be carried out on the production network because of the risk of disrupting clinical activities. The vulnerabilities identified as part of these scans are to be documented and reported to the manufacturer for resolution. If there are any risks identified as part of these scans, they are to be documented, monitored in the risk register and managed or mitigated. **Device malfunctions** Any device malfunction due to vulnerability scans or probing is to be reported to the manufacturer as soon as possible and is not to be connected to a network (whether wired or wireless) or used on a patient until the issue is resolved. If vulnerabilities are found as part of a vulnerability scan and are not documented by the manufacturer, they need to be reported to the manufacturer regardless of their risk rating as the manufacturer is best placed to determine the risk to the medical device and patient. Then these vulnerabilities are to be noted in the risk register as reported to the manufacturer within the agreed timeframes. If there are any risks identified as part of these scans, they are to be documented, monitored in the risk register and managed or mitigated so they will not be reported again following future scans.
Protect	Protecting medical devices	HML43: Where possible, production and legacy medical devices are on a separate network.	**Network segmentation** Medical devices are be isolated on a network separate to the primary organisation network and are not to be connected to the internet unless required. Separating production medical devices from the rest of the network reduces the risk of the medical devices interacting with other devices in an unexpected way. This also prevents them from being scanned for vulnerabilities, which may pose a threat to patient safety. **Access limitations** Limiting access to medical devices reduces the risk of them being tampered by malicious actors. Medical devices are to be protected where possible by: • implementing role-based access control (RBAC) mechanisms • setting up dedicated accounts with strict controls for the personnel within the biomedical technology team who handle medical devices (blocking access after a specific number of wrong password entries, MFA etc.) • establishing physical access control measures for medical device facilities (e.g., by requiring biometrics for access) • setting up a dedicated wireless network for devices that require wireless communication, supported by strict access control and a dedicated access policy • preventing access from public devices • enabling logging and monitoring activities to detect and protect against unauthorised use and anomalies.

Functional Process	Control Area	Requirement	Guidance
			Wireless medical devices Wireless devices are useful to allow patient mobility and impact patient outcomes by allowing physicians access to real-time data on patients without the physician physically being in the organisation and allowing real-time adjustment of patient treatment. The channels through which the information travels to ultimately reach the remotely located care provider open up many security vulnerabilities. Hackers who gain access to the data server could obtain and/or alter information from the device, compromising the patient's confidentiality, privacy, and the integrity of treatment. In addition, hackers within communication range of the device can interfere with its operation, posing serious risks for patient safety. Information being transmitted to and from wireless devices are to be authenticated at all times and encrypted to minimise the risk of tampering and exposure. **Legacy medical devices** Legacy medical devices pose various cyber security risks and sometimes it will be impossible to mitigate these risks, particularly when legacy devices cannot be upgraded to newer operating systems. Wherever possible, legacy devices are to have restricted internet access, isolated where possible from other medical devices and from the primary organisation network. This prevents malicious actors exploiting vulnerabilities in legacy devices to gain access to the rest of the organisation's network.
Protect	Maintenance	HML44: All medical devices are maintained as per the latest updates from the manufacturers and current industry/regulatory standards.	**Manufacturer updates** Updates to any devices are important to prevent security issues, manage security vulnerabilities, and improve compatibility and device features. The system owner and relevant teams are to register for notifications about updates to the devices, to ensure they are alerted to patches for system vulnerabilities as and when they are published. Updates are to be logged and implemented within the timeframes as agreed with the manufacturer and follow documented change management procedures. **Other modifications** Medical devices may undergo modifications such as custom configurations or network changes. Every change introduces risk or modifies the existing risks associated with the medical device. These risks are to be managed and documented in the medical device risk register. The asset register is to be updated if the devices are moved to other parts of the organisation for tracking purposes. Any changes an organisation wishes to make to a device is to be agreed with the manufacturer and is to comply with any relevant regulations for upgrading medical devices. **Remote access** Remote or VPN access may sometimes be required to maintain medical devices. Remote access policies are to set out when, how and why authorised personnel can access the device with MFA and restricting access when

Functional Process	Control Area	Requirement	Guidance
			required. Only whitelisted IP addresses are to be given access to the medical devices. The user activities on these devices are to be logged for investigation purposes to address potential cyber security events. These logs are to be correlated to a centralised logging system where possible, and alerting mechanisms put in place. Remote access to network devices is to be configured so that access and communication is limited to authorised personnel. **Compromised devices** If an organisation suspects a device may have been compromised: • the device is to be disconnected from the network to minimise the threat to the network and to other devices connected to it • the relevant biomedical or technology teams are to be alerted along with the manufacturer for further action. • the device is only be reconnected to the network once the compromise has been dealt with, and biomedical or technology teams have confirmed it is safe to be reconnected. the event is to be documented, along with the steps taken for its resolution • other devices on the network are to be monitored for potential compromise along with the devices with similar configurations from the same manufacturer. • relevant documentation, where applicable is to be updated based on the outcome of the event. **Device malfunctions** Any device malfunction is to be reported to the manufacturer immediately and is not to be connected to a network (whether wired or wireless) or used for patient care until the identified issue is resolved. If vulnerabilities are found as part of a vulnerability scan, and have not been previously noted by the manufacturer, they need to be reported to the manufacturer regardless of the level of risk. The identified risk is to be documented within the risk register and managed or mitigated. Any changes made to these devices are to follow documented change management procedures.
Protect	Dispose or return lease	HML45: Medical devices with patient information are digitally sanitised before their disposal or when they are being returned.	**Removal of patient Information** If a medical device is being disposed of or returned to another provider, any patient information stored on it needs to be deleted first. If devices cannot be digitally sanitised, physical destruction is recommended and a destruction certificate is to be received and stored for reference purposes. **Asset register** Once devices are disposed or returned after a lease, the asset register needs to be updated with their status. **Risk register** If any disposed or returned devices present known or potential risks, the risk register is to be updated to reflect the change in risk.

Functional Process	Control Area	Requirement	Guidance
Detect	Compliance activities	HML64: Medical devices are compliant with relevant standards, and the identified risks are documented within the medical device risk register.	**Compliance to standards** To ensure optimal safety and decrease the level of risk surrounding the medical device, it is therefore imperative that compliance is adhered to. When procuring medical devices, the procurement team are required to perform due diligence by validating the devices against various standards and guidance, including: • US Food and Drug Administration (FDA) guidance for Cybersecurity in Medical Devices • Federal Communications Commission (FCC) • European Medical Devices Regulation • ISO 13485 Medical Devices **Risk register** While performing due diligence, all medical devices are to have their associated risks documented, mitigated or managed and reviewed periodically. **Certification of equipment** Few manufacturers provide certification as part of due diligence activities. When looking at certifications, it is important to understand the scope of the certification to ensure that the devices are suitable. If available online, organisations are to review the vendor certificates and reports including the findings provided by the certification authority along with vulnerability scan reports. These documents are made available to provide assurance on the offered services. Medical device manufacturer documentation is to be reviewed to ensure that the residual risk has been considered in the context of deployment and intended use of medical devices. It is to be noted that the risk is justified and accepted by the organisation management before deployment of the medical device.

Functional Process	Control Area	Requirement	Guidance
Information security governance Implementation of controls in this section ensures that the organisation has the required information structure, leadership, and guidance to meet its security objectives.			
Plan	Ownership of information security	HML12: The organisation's Board or information security steering committee is accountable for organisation's information security governance.	**Information security governance** This is a combination of policies, practices, guidelines, and strategies that align the organisation's personnel and resources to protect information through implementation of security controls and mechanisms. It is important to note that the governance of information security is different from IT security management. Development and implementation of the above ensures that the organisation has the right infrastructure, leadership, guidance, and strategy to mitigate the risks associated with the technology which is being used to provide patient care. The main objective of the governance is to ensure that the security strategies are aligned with the business objectives of the organisation and are consistent with the regulations, needs and expectations of the interested parties. The organisation's Board may nominate an executive to take responsibility for the implementation and maintenance of information security. However, when they choose to delegate their authority to a senior executive at the organisation level or if the position is outsourced, the Board (or the steering committee) still remains accountable for the decisions made by their delegate and determine that any delegated tasks have been correctly performed and budgets are allocated. Effective governance includes: • Board (or steering committee) members understand that information security is critical to the organisation and an update to the group on security performance and breaches is provided every quarter • maintaining compliance with applicable laws, regulations, and in mitigating organisation's risk at an acceptable risk level by performing regular risk assessments • documented and approved policies, processes and procedures comply with the overall business and information security requirements and regular reviews of the enterprise information security are being conducted • annual internal and external audits of the security program are conducted and reported. The results are discussed with the Board, corrective actions are taken in a timely manner and reviewed • a risk management plan is aligned with the organisation's strategic goals, forming the basis for the organisation's security policies and program • a security team comprising of senior management across the organisation from various departments such as finance, information technology, security, risk management, privacy, human resources, communications/public relations, and procurement meet periodically to discuss the effectiveness of the security program, new issues, and to coordinate the resolution of risks and issues • the documented policies and procedures enforce segregation of duties, provide checks and balances, and audit trails against non-compliance or unauthorised access • business, operational and security risks are identified, documented, regularly reviewed and the risk owners accept the risks for their systems and authorise or deny the identified risks • assignment of security risks to respective business owners to manage the risks in the future

Functional Process	Control Area	Requirement	Guidance
			• critical systems, services and digital assets are documented, have designated owners and defined security requirements • zero tolerance for unauthorised changes • personnel are held accountable for not complying with security policies and procedures including reporting any potential security breaches, intentional compromises, or suspected internal violations of policies and procedures • required products, tools and, managed services are purchased and deployed in a consistent and informed manner, using an established, documented process • the goal of the enterprise security program is a continuous risk management and assurance process • documented policies and procedures are regularly reviewed (at least annually or when a substantial change occurs in the organisation), approved, communicated, evaluated and maintained • a security programme is in place to identify, monitor and implement cyber security projects by considering the organisation's business and strategy model.

Identify	Roles and responsibilities	HML27: Roles and responsibilities are defined and documented for planning, implementing, operating, assessing, and reporting on the organisation's information security requirements.	Everyone in the organisation is to understand their role in cyber security governance and resilience. Limited resource availability could make the responsibilities of cyber security fall upon limited personnel. Generally speaking, the below are the identified roles and responsibilities for each tier of management and information security governance.
			
			The Board (or steering committee)
			The responsibilities below are to be carried out by the Board and cannot be delegated:
			• committed and accountable for the organisation's security governance
			• provides strategic direction for cyber security practices and communicates its principles
			• sets priorities by helping to identify critical assets and highlighting the associated risks to provide continuity in patient care
			• endorse the organisation's cyber security policies along with their updates
			• assess performance of the cyber security strategy by:
			  • considering key performance metrics and reporting
			  • reviewing audits and security test reports
			  • reviewing cyber security incidents and near misses.
			
			Senior management (C-suite)
			The management team are responsible for implementation of cyber security strategy while
			• understanding the cyber security strategy by the Board or the steering committee
			• allocating resources for implementation of the strategy
			• approving relevant procedures or standards or guidelines
			• measuring and reporting the delivery of the cyber security programme by identifying and tracking the performance indicators.
			
			If the management is part of the Board (or steering committee), it is important to note that segregation of duties is to be maintained.

Functional Process	Control Area	Requirement	Guidance
			Chief Information Security Officer (CISO) The CISO role oversees the alignment of the governance and security objectives while: • being responsible for establishing cyber security requirements and governance practices • enabling a security framework and architecture for minimal risk and to support scalable business operations (e.g., cloud migration, new region adoption, etc) • leads security team • works with finance, legal, human resources, physical security, infrastructure management • accountable for representing cyber security within the organisation • develops and maintains cyber security policies, procedures and guidelines, including any exemptions that may be needed • provides guidance and leadership on cyber security procedures and guidelines for services, products, operational capabilities, along with the assurance activities that are being performed • develops the cyber security strategy, architecture, and risk management process • manages the budget and funding allocated for the cyber security programme • implements cyber security awareness, training and constantly evaluates organisational cultural security behaviour along with its impact on patient care • assesses cyber security implications to the organisation when adopting new technologies or performing enhancements to the existing ones • guides the organisation on potential consequences and impacts of threats • acts as a point of contact for cyber security • chairs security steering committee (if any) • develops cyber security communication plan • lead audit, assurance and risk management activities • reports to the Board at a minimum of every quarter on the information security key performance indicators. It is important to identify and manage any conflicts of interest, particularly in circumstances where the CISO may hold more than one role within the organisation. In-house knowledge transfer and other mitigation strategies in case of unavailability to ensure the organisational, business, and security requirements are met at all times are to be considered. **Security steering committee** This committee is chaired by the CISO and provides an open forum for all departments to discuss cyber security strategy, policies and procedures, and implementation. This committee consists of various personnel including a few members of the Board, senior stakeholders within the organisation subject matter experts, department executives and other personnel as applicable. These personnel meet regularly while focusing on the direction, scope, budget, timeline, resources and methods which are being used by the organisation to maintain its information security requirements. **Information Security Manager (ISM)** While the CISO focuses on the governance and strategic aspects of cyber security, the ISM focuses on the delivery and operational management of cyber security. This includes: • managing and coordinating the response to cyber security incidents, emerging threats and vulnerabilities • developing and maintaining cyber security procedures and guidelines

Functional Process	Control Area	Requirement	Guidance
			• providing guidance on the cyber security implications of organisational and operational changes • managing the lifecycle of cyber security platforms including design, deployment, ongoing operation, and decommissioning • ensuring appropriate management of the availability, capacity and performance of cyber security hardware and applications • providing input and support to regulatory compliance and other assurance activities, and managing any resultant remedial activity • developing metrics and assurance frameworks to measure the effectiveness of the security controls • providing day-to-day management and oversight of operational delivery. Roles like the Cyber Security Operations Manager focuses on the technical aspects compared to the ISM and is more actively involved in the day-to-day operations of cyber security. A RASCI (Responsible, Accountable, Supporting, Consulted, Informed) model - a simple table is recommended to be defined at the organisation level for defining various cyber security roles for the activities which are to be performed.
Identify	Information security in project management	HML28: Organisations are to integrate information security into project management.	**Project management** Information security is to be treated as an essential consideration in any new or existing project, regardless of the project's complexity, duration or domain area. Considering information security early in the development of the project could help protect information by identifying potential threats, vulnerabilities, information security risks, and implementing appropriate security controls. For effective information security in project management, consider: • information security objectives are part of the business case, identifying the time, effort and budget required for information security and the project objectives • factoring project risk management process within the project lifecycle • performing an information security risk assessment, identified risks are to be treated as per risk treatment plan, and evaluated for effectiveness • adhering to the organisation's documented and approved policies and procedures • creating relevant operating procedure documents supporting the project • providing training to relevant roles within the organisation • logging and monitoring the activities that are being performed on the applications or services which are used to process, store, or transmit information • maintaining compliance with the legal, statutory, regulatory, and contractual obligations to the organisation • performing security due diligence against all components across the project lifecycle. The identified risks are tracked and reviewed at the project governance level and necessary controls are to be implemented to attain an acceptable level of risk. Implementing information security practices within project management helps organisations ensure that their desired output comes with the highest possible level of security. **Security risk assessment (SRA)** A security risk assessment identifies information security vulnerabilities and evaluates how they might be addressed and prioritises them according to likelihood of vulnerabilities being exploited along with their impact.

Functional Process	Control Area	Requirement	Guidance
			Performing an SRA helps the organisation to understand its business functions, operational processes, information systems, threat profile, threat landscape, risk profile and the information it needs to secure. An SRA is typically carried out by a Security Consultant, and often takes place when new IT services or infrastructure are introduced, or when a major change is made to existing services or infrastructure. Identifying and understanding the risks organisations face can help them: • assess and understand the organisation's ability to address the risk • understand whether the organisation is meeting its obligations to its patients, staff, partners and stakeholders • prioritise the work that needs to be done to prevent or mitigate a potential cyber security incident • manage the ongoing risks by understanding, assessing, and evaluating the current risks, controls and their effectiveness and the residual risks as a result of the assessment • to see if contractual and compliance requirements are met • close the security gaps and strategically develop the organisation's security program • reach an informed risk management strategy • agree on residual risk and any control non-compliance that may need to be addressed. • limit uncertainty on what may go wrong with organisational information systems • have better visibility of the information threat landscape. **Security by design** It is an approach to strengthen the cyber security of the organisation by developing a robust information security architecture and their underlying dependencies for any new or current project. It is more of a proactive approach rather than a reactive approach. The principles of software development lifecycle (SDLC) methods are to be documented and followed for any project to strengthen the security of the application of the service which is being developed or enhanced. This approach focuses on capturing and analysing the security aspects and incorporating the security measures throughout the ideation, development and implementation process. It is vital to understand that this approach is not going to fully safeguard the information. However, it aims to enhance the security measures that can reduce the cyber security risks and weaknesses as it requires to investigate the safety aspects from the beginning of the infrastructure and/or application development. The project manager or scrum master is typically responsible for ensuring the IT project team adheres to the security by design principle during the design phase of the project.
Protect	Performance measurement	HML46: Metrics affecting the organisation's cyber security posture are regularly reported to the Board, and any decisions made are clearly documented.	**Measuring effectiveness of cyber security** The cyber security activities are to be accurately measured, assessed, monitored and reported to the organisation management and the Board and any relevant stakeholders regularly (at least every quarter) for its effectiveness. The CISO is to be accountable for this reporting measurement forming part of their responsibilities for information security governance. It is then the responsibility of the Board to decide on: • what measurement needs attention? • what additional activities are to be measured and monitored? • who shall monitor? • how to monitor? • frequency of monitoring • who shall analyse and evaluate the results obtained and its frequency?

Functional Process	Control Area	Requirement	Guidance
			Measurement of cyber security is also performed by testing the effectiveness of the security controls to maintain confidentiality, integrity, and availability of information by the organisation. The evaluation of these security controls can be performed by using a combination of internal and external methods such as: • self-assessments • internal reviews or audits • penetration testing or security reviews • independent reviews or external audits to maintain organisation's compliance requirements. When developing cyber security performance measures, it is important to consider a mix of quantitative and qualitative measures. Organisations are to develop, report on and monitor Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) to assist senior stakeholders in risk and performance measurement and monitoring respectively, and trend analysis projections of the cyber security program. It is also important to develop these measures not only with respect to emerging threats, risks, behaviours but also to the organisation's priorities, strategies and risk tolerance, or the need for further investment. All metrics are recommended to follow the SMART model: specific, measurable, achievable, relevant and time bound. These actions indicate the cyber resilience of the organisation, and progress made through the cyber security programme. Measurement and reporting are vital to good governance, enabling information decision-making and sustainable investment in cyber security. Any indicators which are not meeting their target levels are to be documented and recorded for tracking purposes.

Functional Process	Control Area	Requirement	Guidance
Physical and environmental security Implementation of controls in this section ensures that unauthorised physical access to the restricted areas within the organisation and its information processing facilities are managed.			

Plan	Policies and procedures	HML13: A documented policy and supporting procedures for maintaining physical security within the organisation is in place.	It is important to secure areas of an organisation where information is stored and processed, to guard against both physical threats to information (such as theft, tampering with devices, or patients accidentally wandering into information storage areas) and environmental threats (such as those posed by floods, fires or extreme weather).
			
			Physical and environmental security policy & procedures
			Physical security within an organisation refers to the entire space including all entries/exits, smoking area, car parks, storage areas, and is not to be limited to the front door as they can pose a risk to the organisation. The mechanisms to implement controls for safeguarding physical security is to be supported by a documented and approved policy along with relevant supporting procedures. These documents provide a steer to the team who is developing the procedures to achieve the required outcome. While developing this document, consider:
			• scope and purpose of the document
			• the installed security systems comply with building codes, fire prevention codes, other regulations and contractual agreements
			• provisioning of physical access to all areas of the organisation is to be documented and managed
			• access to all entry/exit points, especially those leading to restricted areas, are to be controlled by access cards, biometrics, pins and similar measures, and how access will be recorded
			• managing the access of visitors or temporary personnel
			• managing and recording access to restricted areas
			• how secure areas are protected against threats such as extreme temperature, humidity, floods, and power failures
			• how new areas or sites will be assessed for physical and environmental security
			• performance of site assessments when acquiring or setting up new areas to provide patient care and process information
			• securely maintain and monitor a physical logbook or an electronic audit trail of access to restricted areas while protecting the logs
			• police vetting for security guards
			• access cards –
			  • are to have photo identification
			  • cards are not to be shared
			  • clear return process for when a staff member ends their employment
			  • lost cards are to be reported immediately and cancelled promptly when they are reported lost
			  • allow an individual to access areas of the organisation they need to visit
			  • access provisioning, modification: the request with a valid reason is to be authorised by the manager and approved by physical security team manager prior providing or modifying the access or moving between departments with different access levels
			  • access de-provisioning: to be included as part of exit process when a person is being terminated or at the end of contract with the organisation

Functional Process	Control Area	Requirement	Guidance
			• access reviews: reviews on access cards are to be performed for all locations by comparing with the active personnel list within the organisation at least every quarter to check if they are still valid. Access to the identified restricted areas is to be reviewed at a minimum of once every month to remove the accesses which are no longer required. Any suppliers having access are to be reviewed with the supplier • utility systems – • all utility systems are to be identified and documented along with respective testing and maintenance requirements which are to be followed • be secured from unauthorised access, and an alarm to be set to warn against malfunctions • emergency systems, lighting, fire suppression, and emergency power systems, are in place and tested regularly to ensure functionality • redundancy is configured for critical utility systems • cleaners – • adequate and appropriate police vetting are to be performed • are assigned a unique identifier that records their access around the facility • able to be identified with the help of uniforms, badges with photo ID etc • access to restricted areas is not provided without prior approval from security • loading/delivery zones – • there are clear procedures for sending, receiving, and screening equipment or parcels • equipment is to be screened before it is connected to the organisation network • receipts for sending and receiving equipment and parcels are to be documented for reference • are secure areas, separate from public areas and with restricted access • monitoring the premises using CCTV cameras, security alarms, guards and keeping a record of the entire movement to provide a complete view especially in restricted areas • backups for access control systems (including but not limited to biometrics, access cards, pins), CCTV recordings configurations are to be performed and tested • any technology changes or enhancements that are being made to the existing physical security mechanisms is to undergo a documented risk management and change management process. Any incidents such as unauthorised access or tampered equipment are to be logged and dealt in accordance with the organisation's documented incident management procedures. Exceptions to the policy or procedure are to be approved by authorised personnel, documented for reference along with an end date for further review or as per the organisation's exception management guidelines. The documented policy and procedures are to be reviewed regularly or when there is a change in the organisation's structure. Exceptions identified are to be approved by authorised personnel and well documented, including a date at which the exception is to be reviewed. Personnel found to have violated this policy may be subject to disciplinary action as per the organisation's documented processes, up to and including termination of employment, and related civil or criminal penalties. The above documented policy or procedure helps in protecting the organisation from physical attacks which can be of various types such as: • accessing restricted/secure areas

Functional Process	Control Area	Requirement	Guidance
			• stealing the organisation's information assets • gaining unauthorised access to organisational assets in restricted areas, which have critical applications or services hosted on the e.g., server room, network rooms, cabling risers/ducts, UPS, generator, building management systems (BMS) – heating, ventilation and air conditioning (HVAC) system etc • ingesting malware onto organisation devices and network ports through unauthorised physical access (e.g., inserting malicious USB drive into a computer or server). **Physical security risk assessments** Risk assessments that identify the potential consequences of physical and environmental threats are to be performed prior to beginning of operations at any location, and at regular intervals. Necessary safeguards are to be implemented and changes to threats are to be monitored and reassessed. Specialist advice is to be obtained on how to manage risks arising from physical and environmental threats such as fire, floods, earthquakes, explosions, civil unrest, toxic waste, environmental emissions and other forms of natural disaster or disaster caused by human beings. Physical premises location and construction are to take account of: • local topography, such as appropriate elevation, bodies of water and tectonic fault lines • urban threats, such as locations with a high profile for attracting political unrest, criminal activity, or terrorist attacks.
Plan	Clear desk and clear screen policy	HML14: A documented and approved procedure to remove papers and removable storage from easily accessible areas is implemented.	Documents containing health and patient information are often extracted and printed for various purposes. Not everyone working within the premises may be authorised to view or know this information, as it might contain personal, sensitive, and/or confidential information. So, it is important to protect such information from being accessed by unauthorised personnel. **Clear desk and clear screen procedures** There is a need for a procedure to ensure that all health and patient information that the organisation holds are always kept secure. The documented procedures are to be adhered to by all personnel who are responsible for storing, processing and transmitting information. The implementation responsibility of this document lies with the managers of respective departments within the organisation. They need to ensure that all materials are removed from workspaces and locked/filed away when not in use or if the personnel are not at their workstation. While documenting a procedure, consider: • all devices – laptops, desktops, mobiles are to be electronically locked when not in use or unattended • information available as hardcopy or in removable storage is either locked or encrypted and is accessible only by authorised personnel if still in use. Otherwise, the information is to be either shredded or destroyed • keys to storage units are not to be left unattended and PINs or passwords used are to be stored in an approved password manager and not written down • documents from printers are to be removed as soon as they are printed • secure printing is to be used to avoid potential disclosure of information • hardcopies of information are to be disposed of as per the organisation's security requirements • boards containing information are to be erased or notes securely disposed off before the area is unattended e.g., whiteboards and flipcharts in meeting rooms • screens displaying information is to be positioned so that they cannot be seen by unauthorised personnel.

Functional Process	Control Area	Requirement	Guidance
			Care is to be taken within the organisation: • to ensure that the organisation's assets are not left behind (e.g., documents fallen behind drawers or furniture) when facilities are being vacated • non-organisation staff i.e., patients are only as close to IT equipment (servers, storage devices, printers, terminals and displays) as physical constraints and clinical processes demand • the screens with information and monitors at the workstations are to be placed such that they are not readable or accessible to unauthorised personnel and certainly not in publicly accessible areas • cables connecting network and/or medical equipment are protected by taking health and safety into consideration.
Protect	Maintenance of physical and environmental security	HML47: Update, protect and maintain the devices installed as physical security safeguards including the utilities.	**External and environmental threats** Areas, buildings, and rooms that house information, its associated assets and processing facilities are to be protected from tampering, unauthorised access and physical damage including floods, fires, leaks, and temperature sensitivities. **Site plan** To determine the different types of threats, one needs to understand the way the facility is designed. To understand how to protect information and assets from these threats, a site plan is to be developed, regularly reviewed and updated. As well as setting out the physical layout of the site and networks such as the electrical plan and surveillance systems, the documentation is to consider: • areas or zones covered within the site • building and design layout including electrical plan and surveillance systems • a summary of the security risk review for the site including possible threats and risks identified, and the implemented security controls needed to manage these risks along with their effectiveness • roles and responsibilities of security personnel • administration, operation and maintenance of access control, alarm systems, and utilities installed along with relevant steps to follow in case of any security events so as to operate in a fail-safe manner in the event of a breakdown • key management, assigning or unassigning access cards, enabling biometrics, personal identification number codes, passwords, etc as applicable • security awareness training and regular briefings • processes for regularly inspecting audit trails and access logs for the implemented security mechanisms • daily inspections and lockups • incident reporting • periodically conduct risk assessment for the facility or upon major changes to the facility • review of this documentation along with its authorisation, approval and communication process. **Maintenance of utilities** It is important to have a thorough understanding of the utilities used in the organisation, and how they are interconnected, as damage or tampering to one system may have major consequences for the organisation as a whole. These utilities may include: • cabling • network ports

Functional Process	Control Area	Requirement	Guidance
			• water sprinklers • fire detectors • temperature and motion sensors • humidity management devices • power generators, backups • surveillance cameras. An overview of the utilities in an organisation is to be developed, regularly reviewed noting their location, their maintenance schedules, responsibilities for updates and checks, and how they can be kept secure from damage, theft or tampering. If outsourced, utility providers are to look beyond gates, fences, and keys to maintain round-the clock security for the organisation's premise. This requires relevant teams to understand the weaknesses, potential threats for the site and the response procedures which are to be followed if there are any suspicious behaviours or potential incidents. **Security of cabling** Cables are used to carry power, voice, data and supporting services. Structured cabling is used to establish an organised path for the connections in maintaining the organisation's infrastructure. Improper installation of cables may lead to potentially damaging the equipment, electrical surges, and fire hazards. A clear cabling structure is recommended to be in place to add or remove components, fix related issues, identify its path to the connected devices. Protecting cables not only keeps cables together but also reduces the risk of trips, slips, damage from water, chemicals that may cause fire or electrical shortages, and reduces signal interfaces. Standardising cabling installations ensures that the cabling system performance is at an acceptable level. While standardising, consider: • shielding: reduces electrical noise and reduces its impact on signals and lowers electromagnetic radiation • labelling: to make it easy for personnel to find the other end of the cable • colour coding: to separate types of cables and to organise and to avoid wrong connections • grouping of cables, access to patch panels and cable rooms • cabling inspection to be performed regularly to detect unauthorised tampering • power and communication cables are to be segregated to prevent interference • measures to protect cables from accidental damage • as applicable, fibre-optic cables are used. In all cases, potential risks arising from cabling incidents or malfunctioning are to be identified and managed.

Functional Process	Control Area	Requirement	Guidance
Protect	Visitor management system	HML48: Secure areas of the organisation are protected from unauthorised personnel.	**Visitor management** A visitor is anyone in an organisation, related facility or at the premises who is not an employee and/or who has been granted access to the facility or area e.g., temporary personnel who work within the organisation on behalf of suppliers. It is important to keep track of everyone who is on the organisation premises and is a visitor. At any given time, this helps guard against unauthorised access to secure areas, and also helps account for everyone in the case of emergencies or evacuations. Relevant procedures based on the organisation's requirements are documented, approved and implemented to allow different types of visitors i.e., patients, utility maintenance personnel, suppliers, etc and the areas within the organisation which they are authorised to visit. **Visitor management system** To manage visitors effectively, either a visitor register, or an equivalent electronic system may be used. Temporary access cards may also be needed for personnel who may need access to certain areas. The visitors are to be authenticated using a valid form of photo ID such as a staff ID or driver's license, and capture: • name and organisation • person visiting, role, and email ID • entry and exit date and time • purpose of the visit • contact number • visitor pass number. Additionally, visitors are to be briefed on emergency exits and evacuation procedures. Multiple visitor registers could be maintained based on the area of the organisation which is being accessed e.g., server room, specialist medical area. Security personnel are to be notified of unescorted visitors unless an exception is granted. Any suspicious behaviour is to be reported as potential incidents and dealt with accordingly. If an electronic visitor management system is used, care is to be taken such that: • the device is not stolen or tampered with • devices are assessed for security risks before being connected to the organisation network • identified security risks are mitigated before implementation of the system and/or device • the device is maintained with security patches • appropriate training is provided to personnel maintaining the device, such as the technical team and reception staff • controls are in place to mitigate against potential physical or logical threats **Temporary access cards** Access cards are issued for a limited amount of time (i.e., just-in-time access) for visitors to use during their visit are to be kept separately. A review of the temporary access cards is to be performed at the end of each day. Any missing cards are to be disabled immediately, and access logs are to be checked for unauthorised access or tampering.

Functional Process	Control Area	Requirement	Guidance
			Secure or restricted areas Areas such as server and/or network room, laboratories, medicine storage areas, and areas restricted for doctors are to be closely monitored and only accessible by authorised personnel. Entry to these areas is to be controlled by access control mechanisms such as biometrics, PINs, access cards, lock and key etc. Access is to be provided to authorised personnel only and for a restricted amount of time based on the business and security requirements. Access reviews are to be performed such that access is provided to authorised personnel only and logs are to be protected from unauthorised access or tampering, regularly reviewed to check that there was no unauthorised entry, access or tampering. These areas are to be further monitored via surveillance cameras for suspicious behaviour.
Detect	Monitoring of physical and environmental security mechanisms	HML65: Installed physical and environmental security mechanisms are monitored for potential security incidents.	**Continuous monitoring** Physical premises and restricted areas within the organisation are to be continuously monitored by surveillance systems, security guards, alarms, CCTV and other management software(s). These services are either managed internally by the organisation or outsourced to a service provider. Access to restricted areas within the organisation are to be continuously monitored to detect unauthorised access or suspicious behaviour. Various mechanisms such as those below are to be used to protect the organisation from physical and environmental threats that are identified: • CCTV to detect suspicious behaviour • access controls mechanisms to detect unauthorised access (i.e., contact, sound, and motion detectors, etc) • different types of sensors to detect temperature, fire, humidity levels, water levels • duress alarms for any protests or civil unrest. The implementation of monitoring systems along with their design plans are to be kept confidential to protect the organisation from potential security incidents which could go undetected, theft, damage, or tampering. Care is to be taken to protect monitoring systems from: • unauthorised access to prevent loss of information which is being recorded or collected • being disabled remotely by malicious users • be protected from tampering and are to be regularly tested to ensure that it is working as intended. The information which is being recorded are to be stored, backed up and archived according to the organisation's data retention requirements, while also complying with regulatory requirements.

Functional Process	Control Area	Requirement	Guidance
Remote working Implementation of controls in this section ensures that information is protected when personnel are working from remote locations.			
Protect	Remote working requirements	HML49: Secure mechanisms are available and supported by a documented policy or guidelines to connect to the organisation's network.	**Remote working** The practice of personnel doing their jobs from a location other than the one provided by the organisation is termed remote working. With modern technologies and devices, remote working has become important to support flexible ways of working and in response to events that prevent from working from the organisation. However, in a healthcare environment, it is challenging for clinical roles to assess, treat and look after patients remotely. If an organisation allows remote working, it is essential to set approved and well documented guidelines for how those roles handle information. **Remote working procedures** The health sector deals with sensitive health and personal patient identifiable information whose security is to be maintained. Roles for which remote working is allowed are to be supported with guidelines and procedures which are to be followed. While designing this document, consider: • use of encryption with multi-factor authentication and conditional access control to login remotely to the organisation's network • information is encrypted and transferred only via authorised individuals, approved channels, processes, and technologies • approved devices are to be used to access information • the services that are being provided • all applications, supporting services and the devices are maintained with latest patch updates • information is not downloaded or stored on personal devices • use of software on organisation issued devices to enforce settings and organisations policies i.e., remote wiping, device tracking, application installations, accessing only authorised resources, etc • physical security of the devices • devices to be accessed by authorised personnel only and passwords or passphrases are not stored in clear text • home or public networks are to be protected by strong authentication i.e., PIN or password. Unless otherwise specified, a staff member's manager is to authorise the use of organisation issued devices from remote locations and approved by the business owner listed in the asset management register. The risks of using these devices outside the organisation network are to be documented within their organisation's risk register, and these risks are to be mitigated and managed by implementing security controls. If any abnormalities are found on the devices, they are to be logged as a potential security incident and managed accordingly. **Remote working guidelines** • appropriate training and guidance are to be provided to personnel who have been approved to work remotely. • only authorised organisation devices are to be used

Functional Process	Control Area	Requirement	Guidance
			• the type of organisation and information, applications, systems and services that require authorisation for access are identified • means of connecting securely to the organisation network • business continuity procedures if any applications are not accessible • securing the devices by locking the screens when not in use • ways to report suspected tampering with devices • ways to recognise and deal with spam email and malicious links • not allowing family or friends to use organisation issued devices • patching, backup schedules, antivirus and firewalls are not terminated • ways to connect organisation issued devices to authorised printers • ways to securely dispose of printed material • return of equipment at the end of contract termination or upon change of role that does not require remote working.

Functional Process	Control Area	Requirement	Guidance
Web security Implementation of controls in this section ensures that the web applications which were hosted by or on behalf of the organisation are secure.			
Protect	Security of web applications	HML50: Security controls are implemented if the organisation is developing the web applications to protect them from potential cyber-attacks.	**Web applications** A web application (web app) is a software program that can be accessed over the Internet through any browser interface. Due to an increase in cyber-attacks and data breaches, maintaining security in web applications is a real concern. As web applications become critical, complex, and connected, the difficulty of achieving its security increases exponentially. **Web security** Implementing security measures to protect websites against cyber-attacks, from malicious users, to maintain confidentiality, integrity, and availability of the information on the website is known as web security. Due to the increasing use of online tools and technologies to provide better patient care and to make personal patient information available, there are a lot of web applications which are being developed or used by organisations. To protect patient information from malicious users, consider: • only authorised personnel have access to information stored on the website • use of Web Application Firewalls (WAFs) to provide defence-in-depth protection against application specific threats • the latest version of TLS and other protocols as required are used to authenticate and encrypt information • use of conditional access policy to limit access to web applications from a specific location, IP range, or web-client, etc to reduce some of the attack vectors • secure-by-design and secure-by-default strategies to tackle the software development cycle (SDLC) • security controls and mechanisms are in place to protect against the OWASP top ten most critical security risks to web applications • only fully supported browsers and email clients are allowed, kept up to date with the latest version of browsers and email clients provided by the supplier • restrict, either through uninstalling or disabling, any unauthorised or unnecessary browser or email client plugins, extensions and add-on applications • performing penetration tests against OWASP top 10 and configuration reviews before the website or web application goes live • continually monitor for malware, phishing, and other kinds of cyber-attacks etc which could lead to information loss, tampering or unauthorised disclosure. Implementing these measures can: • protect organisations by preventing loss, tampering or unauthorised disclosure of personnel, patient and organisation information • protect organisations from negative legal, financial or reputational exposure • reduce or limit exploitations and injection of malicious code • provide continuous and better healthcare experience for patients • help meet the organisation's security and business objectives • help comply with regulatory, statutory, and legal requirements.

Functional Process	Control Area	Requirement	Guidance
Compliance Implementation of controls in this section ensures that relevant legal, regulatory and contractual requirements are met.			
Identify	Compliance requirements	HML29: Relevant legal, regulatory and contractual requirements are identified and implemented.	**Compliance** There are a range of laws, rules and regulations that organisations are to comply with. Adhering to these along with contractual requirements help organisations in meeting various controls to protect the confidentiality, integrity and availability of information. This can be achieved by implementing security controls, along with policies, procedures, guidelines and best practices. These laws, regulations and contractual requirements are to be considered whenever: • policies and procedures are being developed • security controls are being designed, implemented or modified • roles and responsibilities relating to information security are being determined or modified • information security requirements are being documented for suppliers • information security risk assessments are being performed using the organisation's risk assessment methodology • information security risk treatment activities are being performed • contracts and master service agreements are being drafted for the products or services which are being outsourced to a supplier • information is being stored in other countries and its encryption requirements • cyber insurance is being acquired or claimed • while developing any in-house application to process, store or transmit information by protecting the intellectual property of the code developed • data retention and archival requirements are being defined • incident response plans are being developed • information breach response procedures are being developed. These policies and processes, standards, guidelines, contracts, requirements are to be reviewed periodically so that they continue to comply with the relevant laws, rules and regulations.
Detect	Review of compliance requirements	HML66: Regular reviews are performed to confirm that the legal, regulatory, statutory, and contractual requirements are met.	**Compliance reviews** Compliance reviews help organisations confirm they are meeting relevant legislative and regulatory requirements, and to identify any gaps compared with international best practice(s). As well as ensuring the security of information, these reviews help organisations minimise potential security incidents, and avoid fines, penalties, lawsuits or in the worst case, loss of patient life or organisation closure. When performing a compliance review: • identify the list of requirements, applicable laws, statutory stipulations, and regulations to comply with • clearly document the compliance process and ways to continuously assess and maintain compliance • monitor the changes to the laws, regulations, agreements, requirements and determine if they apply to the organisation • track the identified changes and prepare an implementation plan so that they are reflected in the organisation's documented policies, procedures, guidelines, etc

Functional Process	Control Area	Requirement	Guidance

			• communicate the implemented changes which are being performed to relevant personnel.
			
			Review of policies, procedures and other relevant documents
			To maintain compliance, the developed documentation is to be reviewed to ensure that it stays current. It is the responsibility of the managers, service owners, product owners within the area to identify the gaps and update the documentation accordingly such that the compliance requirements are met. If any change is to be performed on any product or service, the organisation's change management process is followed. The performed changes on the documentation and/or to the product or service is to be communicated to relevant stakeholders in a timely manner.
			
			Planning an audit
			Organisations are to develop and maintain processes to conduct independent reviews of their security posture. While these reviews are initiated by management, the audit team is to be independent, and appropriately skilled. The results of these reviews are reported to management, and the findings from these reports are be recorded and a remediation plan is developed to mitigate the identified issues.
			
			Reviews are to be performed regularly and/or when there:
			• is a change in the organisation's strategy
			• are structural changes to the roles within the organisation
			• is a change in the leadership
			• is a merger or acquisition
			• is a change in the information security objectives and/or requirements
			• is IT infrastructure that is introduced e.g., cloud migrations, new deployments or if there is a significant change in the existing IT environment
			• is a change in contractual requirements.
			
			Review of compliance can be performed in various ways such as:
			• internal audits: internal (inhouse) audits are to be performed periodically to review the organisation's adherence to the documented requirements. These audits are to closely evaluate the requirements by validating or reviewing associated policies, procedures, and guidelines and the way they are implemented within the organisation for compliance. The reports generated helps the organisation to prepare for formally conducted external and compliance audits which are conducted by independent parties.
			The internal audit function is responsible for:
			  • assessing cyber security risks against the organisation's strategy, business and security goals
			  • conducting risk-based cyber security assessments against the organisation's technology, people, and processes
			  • assessing the organisation's compliance against cyber security regulations, contracts, other legal and statutory requirements
			  • reporting and escalating risks to management for mitigation.
			• external audits: these audits are performed by independent parties, provide a general overview of the organisation's security posture, to see if the findings identified are aligned with the claims made by the auditee organisation. The generated report is usually not as detailed as an internal audit report.

Functional Process	Control Area	Requirement	Guidance
			Components of an audit Typically, an audit consists of: • interviews with relevant key personnel and stakeholders • the observation of a control execution • reviews of records such as documented policies within the organisation • assessments of the knowledge/competency of the organisation's security personnel • assessment of physical and environmental security measures • reviews of penetration tests, technical reviews, service reports obtained from the suppliers • reviews of the implementation plan developed from any internal audit findings. **Self-assessment** An assessment on the compliance requirements to determine the security posture of the organisation can be performed. While performing a self-assessment, consider: • mapping internal controls and their compliance to external frameworks, standards, contractual, legal and statutory requirements • security policies, procedures, standards and guidelines are documented, approved, communicated, implemented and reviewed • independent audit and assurance assessments are conducted according to relevant standards at least annually and contractual agreements, etc are documented and considered • independent audit and assurance assessments are performed according to risk-based plans and policies • an audit management process that includes planning, risk analysis, security control assessments, remediation activities, review of previous reports and supporting evidence is defined and implemented • personnel's security awareness training is reviewed regularly and conducted for all relevant personnel.

Functional Process	Control Area	Requirement	Guidance
Cloud security Implementation of controls in this section ensures that the risks raised with the use of cloud services are managed.			

Plan	Cloud security policy & cloud security agreement (CSA)	HML15: Organisations have planned maintenance of information via cloud services as per documented policies and agreements.	**Cloud security policy**
			Cloud security is the practice of protecting cloud-based information, applications, and infrastructure from cyber-attacks and cyber threats. As enterprise adoption of cloud services increase, business-critical applications and associated information is being migrated to trusted third-party cloud service providers (CSPs). Although most major CSPs offer standard cyber security tools with monitoring and alerting functions as part of their service offerings, in-house IT security personnel may find that there are gaps between what is being offered in the CSP's tools and the organisation's requirements.
			
			The development of a cloud security policy helps the organisation's management to balance the benefits of adopting cloud services with an acceptable level of information security risk. This further reduces the risk of information being lost or breached, avoids non-compliance, reputational damage, fines, maintain business continuity and availability of information as required.
			
			While developing a cloud security policy, the organisation is to consider:
			• the purpose and scope of the policy
			• cloud service provider selection criteria and risk management
			• cloud service provider contractual and data processing agreements
			• what information can be uploaded to the cloud and how it is to be protected
			• the information security risks for each type of information asset and how they are to be mitigated
			• who is authorised to use cloud platforms and the constraints (e.g., legal and organisational) they operate under
			• use of multi-factor authentication
			• enforcement of conditional access policies
			• use of cloud services and conformance to its compliance objectives
			• information security incident management
			• logging and monitoring of all events based on threat modelling
			• documentation of all information security controls that are managed by the CSP and the controls that are managed by the organisation
			• obtaining assurance on information security controls that are implemented by the CSP
			• managing changes in services that are being provided by the CSP
			• portability and interoperability between the services within the organisation
			• policy compliance measurement, exceptions, non-compliance, and continual improvement
			• whether the cloud service provider:
			  • had undergone a CSA STAR certification and/ or attestation
			  • would allow the organisation to review a recent third-party audit report (i.e., ISO 27001 or SOC 2 Type II) that include assessment of controls and practices related to virtualisation and separation of organisation information
			• modifying or terminating the use of cloud services including exit strategies.

Functional Process	Control Area	Requirement	Guidance

			Cloud service agreement (CSA)
			CSAs are used to set clear expectations for service between the organisation and the CSP from a service, security and commercial point of view. The CSA protects the organisation's access to information, minimises the expense of any required remedial action, and specifies what happens in the event of service interruption and any penalties.
			
			Although every CSA is different, it will usually cover three areas:
			• customer agreement
			• acceptable use policy
			• service level agreement
			  • confidentiality and availability of information
			  • information access, retention, protection and removal requirements
			  • performance objectives
			  • roles and responsibilities for the services being covered
			  • incident handling
			  • security requirements along with business continuity
			  • policy and compliance requirements by obtaining independent assessment reports
			  • service management requirements
			  • effective governance process(es)
			  • fines and service credits
			  • supply chain management
			  • exit process.
			
			Before negotiating or signing a CSA, the organisation is to obtain legal and technical security advice, as cloud services usually involve multiple service providers who may or may not be legally bound to the organisation. A robust CSA is important to protect the rights of the organisation and to ensure there is no misunderstanding between the parties.

Identify	Cloud security risk assessment and assurance	HML30: A risk assessment methodology and cloud assurance activities that support the use of cloud technologies are in place.	**Risk assessment methodology** Organisations may take a proactive and repetitive approach to address information security concerns around the information which they hold. A documented risk assessment methodology or processes helps them to: • identify the hazards • assess the risks • mitigate the risks • record the findings • review the implemented controls. **Risk assessment matrix** A risk assessment matrix, also known as a probability and severity matrix is a tool used for risk evaluation. Depending on the likelihood and severity, risks are to be categorised as extreme, high, moderate/medium, or low. As part of the risk management process, organisations use risk matrices to help them prioritise different risks and develop an appropriate mitigation strategy. Typically, a matrix will: • identify the risk profile – strategic, operational, financial, reputational, legal and external

Functional Process	Control Area	Requirement	Guidance

			• determine the risk criteria – likelihood, impact
			• assess the risks – extreme, high, moderate or medium, low, very low
			• prioritise the risks and implements a mitigation strategy.
			
			It is important to note that organisations may have their own risk rating levels that are different than the ones mentioned here, to evaluate their own risks.
			
			Performing security risk assessments (SRA)
			A typical SRA is performed based on the criticality of the information which is being managed or processed by the application or service based on the results from the business impact analysis (BIA) as explained in the business continuity and disaster recovery domain.
			
			Organisations are to periodically carry out an SRA on new and existing systems, applications to understand their risk profile or when any system changes are being introduced. Ideally, an SRA is to be carried out every two years. When carrying out an SRA, there is to be a representation from all departments where there are vulnerabilities., and an effective consultation and communication among all stakeholders.
			
			An SRA typically involves:
			• risk identification:
			  • identify potential threats, such as natural disasters, hardware failure, malicious behaviours i.e., performing threat modelling
			  • identify vulnerabilities including software, physical and human vulnerabilities i.e., performing a vulnerability assessment
			• risk analysis:
			  • analyse the implemented organisation's and security controls, determine the likelihood of the identified risks along with its consequence
			  • determine the controls (deterrent, preventative, detective and corrective) to mitigate or manage the risk
			  • document the results to develop a risk assessment report which is acknowledged by the business owner (and risk owner unless they are not the same personnel)
			• risk evaluation: evaluate the risks against the organisation's tolerance levels i.e., risk profile
			• risk treatment: select, implement and evaluate the effectiveness of controls which modifies the risk status (accept, treat, avoid, transfer) of the documented risks in the risk register
			• risk treatment plan or security risk management plan (SRMP): once the treatment for the risks is selected, it is the process of implementing those treatments which includes the implementation details of action plans as documented and approved. This could be applicable to individual systems or applications processing or storing information or a single plan for the organisation covering all information processing systems or applications
			• system security plan (SSP): contains details of system description, system boundary, architecture, and security controls in one document along with the details on how all the security controls are implemented
			• monitoring and review: continual assessment of risks to ensure that the selected treatment remains effective. This ensures that likelihood has not increased and to ascertain if the cost of the control(s) to reduce the impact has decreased to a level that makes its implementation affordable

Functional Process	Control Area	Requirement	Guidance
			• communication and consultation: effective communication between stakeholders is to ensure that risks are understood and decisions about risk response selection are appropriate. While performing a risk assessment, risks associated with both internal and externally hosted systems, applications and services are to be considered along with ICT supply chain risks. ICT supply chain risks are managed through the procurement process, technical checks and control assessments. Any changes which are being performed to the service or system or application as a result of risk assessment process is to follow the organisation's documented change management procedures. **Cloud assurance activities** Organisations are to perform due diligence activities on services provided by the Cloud Service Provider (CSP), not only before they are onboarded but also during the service period and when there is a change in the system or service or application. As the CSPs are responsible for their infrastructure, platform and software based on the services obtained by the organisation, organisations are accountable for the risks and implications they may endure as a result of using the services from the CSP. Independent assurance reports such as service organisation controls (SOC) 2 reports, ISO certifications or compliance reports could be obtained from the CSPs to understand their operations and compliance status against various international standards and best practices. Additionally, a latest copy of the consensus assessment initiative questionnaire (CAIQ) self-assessment can be obtained from the provider through the Cloud Security Alliance (CSA) Star Registry. While reviewing the reports, it is important to note that the services which are being acquired by the organisation from the CSP are within the scope of the report.
Protect	Cloud security architecture	HML51: The organisation's architectural strategy supports the adoption of cloud technologies.	**Cloud computing** The on-demand availability, elasticity, and scalability of computing power without direct management by any personnel is known as cloud computing. These internet technologies provide access to storage, files, software and devices that are used to process, store and transmit information with the help of the internet. **Cloud computing services** Use of cloud computing technologies and services is more flexible and reliable with increased performance and efficiency. Delivering these services are categorised into: • Infrastructure as a Service (IaaS): service that offers on-demand virtualised computing resources such as storage, networking over the internet from a cloud service provider (CSP). The CSP is responsible for maintaining and managing the infrastructure while organisations manage the platform, data, software and pay only for the resources which they consume • Platform as a Service (PaaS): service that offers a flexible, scalable cloud platform to develop, deploy, run, and manage applications from a CSP. The CSP is responsible for updating and maintaining hardware, software, and development tools. Applications are built directly on the PaaS system and can be immediately deployed once they are completed

Functional Process	Control Area	Requirement	Guidance
			• Software as a Service (SaaS): service that offers applications over the internet by a CSP. The CSP is responsible for maintaining and managing the infrastructure, platform and software. • Function as a Service (FaaS): this service is also known as serverless computing. In serverless computing, cloud applications are split into smaller components called functions. These functions are run only when required and are billed based on the usage. They are called serverless because they don't have to run on specific dedicated machines. Serverless functions can scale up easily based on demands. **Cloud computing deployments** Based on where the cloud servers are and who manages them, the cloud computing environment is classified into the following types: • Public cloud: is a cloud computing service provided by a CSP that may include multiple servers, data centres and software. In this case, the computing facilities could be shared by individuals and multiple organisations. Even a single physical server may be shared by multiple tenants using the virtualisation technology • Private cloud: is a set of servers, a data centre or a distributed network, which is solely operated for one organisation, whether managed internally or by a third party and hosted either internally or externally • Hybrid cloud: is a combination of public and private clouds. In this case, organisations may use a private cloud to store and process their critical information and a public cloud for their other services. Some may even use a public cloud as a backup of their private cloud • Multi-cloud: is a kind of deployment where multiple public cloud computing services in a single heterogeneous architecture from multiple suppliers are used. It differs from hybrid cloud in that it refers to multiple cloud services rather than multiple deployment modes (public, private, legacy) instead of a mixed computing environment where applications are run using a combination of computing, storage, and services in different environments - public clouds and private clouds, including on-premises data centers or edge locations • Community cloud: is a shared cloud computing service that is used by a limited set of organisations or personnel. **Cloud adoption strategy** Due to the different types of cloud computing deployments, organisations are to have a strategy in place to improve the scalability of internet-based services while reducing cost and risk. To achieve this, organisations can use cloud computing to store, manage and process information via cloud services such as SaaS, PaaS, IaaS, FaaS. Adoption of a cloud strategy helps organisations to store information in the private cloud while leveraging the technological resources from the public cloud to run applications relying on information. **Cloud security risk assessments** Use of cloud technologies introduces risks to organisations. The potential security risks are to be identified prior onboarding these services so that appropriate security controls are implemented to manage or mitigate the risks. While performing the risk assessments, organisations will: • follow the organisation's documented risk methodology • identify the risk of unavailability of the cloud services including its interoperability is to be considered during the design phase.

Functional Process	Control Area	Requirement	Guidance
			Identifying and understanding the risks organisations could face can help them: • prioritise the risks which are to be mitigated or managed to prevent a potential cyber security incident in a cost-effective manner • review the implemented security controls and decide the need for additional controls • understand the organisation's ability to address potential security threats and/or vulnerabilities • determine if contractual and compliance requirements can be met • close the gaps and strategically develop the organisation's information security program • make risk-based decisions on whether to either treat or accept the risk • build products or applications with security-by-design and by default. **Content delivery network (CDN)** Content delivery or distribution network is a group of servers which are geographically distributed and interconnected for faster web performance, and security for web properties. The CDN uses the organisation's cloud service provider's network to accelerate response times for their websites and applications and also helps organisations seamlessly handle seasonal spikes in traffic. This helps to increase availability of services to organisations. Implementation of CDNs could introduce a risk of a side channel attack being performed, where attackers observe for information leaks that help them break into the cloud service. This can be prevented via restricting access to the origin server's IP address to the CDN and using an authorised management network, which are to be identified during the architecture phase for implementation.
Protect	Use of application & programming interface (API)	HML52: Organisations are to make use of developed and configured APIs for secure transfer of information between different cloud components.	**Cloud API security** Multiple cloud services used by an organisation can be linked together. Cloud application programming interface (Cloud API) enables applications to communicate and transfer information between different cloud services. Cloud API security is the practice of protecting the implemented APIs between cloud applications from cyber-attacks to preserve its confidentiality, integrity, and availability (including the information it processes and transmits over the cloud network and the wider internet). This affects the service and the information it processes and transmits over the cloud network and the wider internet. Proper API security measures ensure that all processed requests to the configured APIs are valid, from legitimate sources, and all responses from the API are protected from interception, tampering or exploitation. **Best practices** As cloud APIs involve communication between several cloud applications, the communication mechanisms are often prone to different type of cyber-attacks such as stolen authentication credentials, man-in-the-middle attack, code injections, and denial-of-service (DoS). To prevent these attacks and protect information, some of the cloud API security best practices include: • enabling secure or robust authentication and authorisation i.e., OAuth2 for SSO with OpenID connect, request-level authorisation • validating all requests • encrypting all requests and responses • only include necessary information • throttling API requests and establish quotas

Functional Process	Control Area	Requirement	Guidance
			• logging API activity • using code that is from a trusted third-party or libraries • conducting security tests • implementation of a zero-trust model and re-authentication for all API calls i.e., not permitting session persistence and cookie-based sessions etc • having web application firewalls (WAFs) and API gateways to filter traffic • setting appropriate identity and access management (IAM) permissions to API keys i.e., development environment synchronising code with the cloud through set API keys.
Protect	Cloud security controls	HML53: Organisations are to ensure that appropriate controls are implemented to protect information in a multi-tenant cloud environment.	**Multi-tenant environment** Using the same CSP computing resources allocated to multiple customers at the same time is known as a multi-tenant environment. This type of architecture is commonly seen in many types of public cloud computing including IaaS, PaaS, SaaS, and FaaS. To ensure that information is protected, the organisations are to recognise the threats, vulnerabilities, and implement defences and evaluate their effectiveness to complement the cyber security measures offered by their CSPs. This can be performed by the following control types: • preventative controls: these controls address the vulnerabilities in cloud services to strengthen the cloud's resilience to attacks by removing security flaws. These are critical in strengthening the service • deterrent controls: these controls are more like a warning system to malicious users but do not protect the cloud environment • detective controls: these controls detect and respond to potential or actual security threats or events • corrective controls: these controls minimise the after-effects of an attack to limit the damage caused by the event. Implementation of these controls help organisations to: • meet legal, statutory, and regulatory requirements • monitor and evaluate the configured cloud services • integrate security-by-design measures to cover cloud supply chain risks • improve compliance practices • share responsibilities and commitment with the CSP • continuously assess and improve security of cloud services. To reduce the risks identified while performing the risk assessments, centralised visibility is to be provided to the security teams via logging and monitoring activities. **Shared responsibility model** This model represents the documented responsibilities that are shared between the organisation and the CSP for securing the cloud environment including infrastructure, platform, software, and other implemented security controls to protect information. In general, while using SaaS services, organisations are responsible for user accounts and identities to form a secure basis for controlling access to resources. Additionally, organisations are responsible for protecting

Functional Process	Control Area	Requirement	Guidance
			information which is hosted using cloud services throughout its lifecycle while implementing appropriate controls to: • retain control over information • ensure cloud service provider has no visibility over information • protect proprietary applications, services and information from unauthorised access • manage its identity and access management.

Functional Process	Control Area	Requirement	Guidance
System acquisition, development and maintenance Implementation of controls in this section reduces the risks during: • procurement • development practices • maintenance of existing technology services.			
Plan	Security while developing applications, products or services	HML16: Information systems are securely designed, and appropriate controls are implemented.	**Security engineering principles** When developing new applications, products and services, it is important to consider cyber security from the outset. Security engineering is the process of incorporating security controls into an information system development lifecycle so that the controls become an integral part of the organisation's operational capabilities. These support the delivery of developed systems including applications or products or services within their risk tolerance and ensure that information is protected while in transit or at rest. Security engineering principles are guidelines for building information security into all architectural layers, in order to have them implemented in a real-world environment they are to be followed by a procedure that is easily understood by all stakeholders. It is important to know that principles apply to every phase of your project's development lifecycle, and to all architectural layers of your final products (including business, data, applications and technology). The developed and introduced principles within the organisation are to address their current situation and identified threats while integrating with the security architecture. So, these principles are to be applied for new and existing systems which are undergoing major upgrades even if the development activities are being outsourced via contractual agreements. Any new technologies which are being used are to be analysed for potential business and security risks. The security engineering principles and the established engineering procedures are to be regularly reviewed to ensure that they are meeting the organisation's security objectives. While developing the security engineering principles, consider: • developing layered protection i.e., defence in depth • establishing strong security policy, architecture, and controls as the foundation for design i.e., secure by design • incorporating security requirements into the early stages of system development lifecycle to identify potential information security vulnerabilities • documenting all decisions made during the system development lifecycle to inform management about security considerations during all phases of the development • information interoperability and integration at various system levels • clearly state physical and logical security boundaries including data sovereignty • qualified and skilled professionals assigned to tasks throughout the product development lifecycle • perform threat modelling to identify use cases, threat actors, attack vectors, and attack patterns as well as introducing compensating controls and design patterns that are needed to mitigate risk • perform a comprehensive risk assessment to identify existing processes, threat landscape, controls in place, and gaps to build a plan to mitigate and manage identified risks • system patching and hardening • adoption of zero trust principle

Functional Process	Control Area	Requirement	Guidance
			• protecting information while in transit and at rest. **Secure coding** Software and applications are to be developed in a way that guards against known or potential security vulnerabilities. Coding guidelines are to be developed to prevent potential vulnerabilities and to protect the confidentiality, integrity and availability of information. This ensures that the code written by various developers is clear, stable and can be easily maintained thus reducing the risk of human errors. It is also important to develop a process for auditing (manual or automated) written source code to identify errors i.e., source code review. While documenting the standards for both new and enhancements which are being made to the technologies, systems, applications, products or services which are being used, organisations are to consider: • implement security principles to guide the development of in-house and outsourced projects • create a well-documented checklist for code review e.g., OWASP code review guide • categorise security vulnerabilities based on the risk identified • usage of both manual and automated approaches or tools • there is continuous monitoring and debugging for early identification of potential security incidents or vulnerabilities • use and maintenance of automated tools for development and security • identify and assess potential threats because of the introduced code • use of separate environments while maintaining segregation of duties and relevant permissions • perform testing during and after development to identify security vulnerabilities • perform regular code reviews, code to be protected from unauthorised access • administrator access to the code is to be protected using additional security mechanisms such as MFA • code is protected and regularly monitored for a variety of vulnerabilities that are introduced by poor design and coding, such as database injection and cross-site scripting attacks. If code is being developed in-house, a Continuous Delivery model is to be used. This helps create a full CI/CD integration that can help detect code defects including potential security vulnerabilities as early as possible, and to ensure they can quickly release properly tested updates before they go into production. It is important to note that this is orchestrated across all environments. **External tools and libraries** If code is being developed using external tools and libraries, it is important to consider that: • tools and libraries are downloaded from a reputable source • tools and libraries are regularly updated • licensed versions are used, and security precautions are taken. All developed code is to be tested and monitored for potential vulnerabilities before its deployment in production environment. Security vulnerabilities identified are to be documented and follow the organisation's documented incident management process. Any changes made to address vulnerabilities are to follow the organisation's documented change management procedures.

Functional Process	Control Area	Requirement	Guidance
			New acquisitions Organisations are to document their business and security requirements when acquiring or upgrading systems, services or applications and consider: • supporting the organisation's identity mechanisms • stores and protects audit logs as per business and security requirements • audit logs are traceable and could be shared to a centralised location for better correlation of events • abnormalities to information access or flow can be reported • performing risk assessment to identify and address the risks • scheduling backups and testing respective restoration procedures • documenting, monitoring and periodically reviewing the identified exceptions • reporting potential incidents and the process for handling them. **Outsourced development** When organisations outsource their software development, it is important to document: • expectations around the development process • how suspicious activities will be monitored • how security incidents will be reported and • how supply chain risks will be managed. Additionally, while documenting contractual agreements, consider: • use of only licensed, supported and latest (as applicable) versions of products • security requirements are identified and monitored throughout their lifecycle • right to audit, or checks on the status of the identified security requirements in the form of independent third-party assurance reports • independent security reviews are performed, and a process for how the threats identified are resolved or managed • provision of threat model as required • information retention and deletion clauses to ensure compliance with legal, statutory, and regulatory requirements • escrow agreements • exit clauses including portability and interoperability of information.
Identify	Business and security requirements	HML31: Business and security requirements are identified, documented and approved when developing or acquiring applications.	**Business and security requirements** A product evaluation scheme is to be developed and used whenever an organisation is considering a new system or service or application, etc. This scheme is to cover: • purpose and scope • suppliers' financial stability and jurisdictional considerations • independent third-party assurance reports • risk based approach that is both user experience and system centric • security functionality • impact on business and security architecture

Functional Process	Control Area	Requirement	Guidance
			• alternative product options • in-house development or off-the-shelf purchasing, or outsourced development • data sovereignty, interoperability, retention, deletion, and portability. Once new system or software requirements are identified, the completed evaluation scheme including documentation of justification for the selection of systems, provides greater assurance than those systems that are still undergoing evaluation or have not completed any formal evaluation activity. Once the preferred is selected: • business and security requirements are to be documented • a formal risk assessment to be performed to understand the risks which the new system or software might introduce to the existing environment containing information • identified risks are to be recorded in the organisation's risk register and monitored for treatment. While performing evaluation (prior to acquisition), organisations are recommended to review the documentation (e.g., terms of use, privacy policy, consumer guides, data sovereignty, right to audit, etc) related to the system and respective independent reviews performed. Non evaluated systems or software downloaded from websites over the internet can contain malicious code or malicious content that gets installed alongside legitimate software may lead to ransomware attacks potentially compromising the organisation's environment. Organisations will need to confirm the source and the integrity of the software they are installing before deploying it in the environment to ensure that no unintended software is installed at the same time. When a non-evaluated system is purchased (e.g., laboratory equipment, devices, etc), organisations are to determine if the equipment has arrived in a state that they were expecting it to and that there are no obvious signs of tampering. A documented report of delivery date, time and source is to be stored as a record for future reference. Security and policy requirements are to be considered when entering into a leasing agreement for equipment to avoid potential information security incidents during operations, maintenance, repairs, or disposal processes. Technical vulnerabilities identified during the use of the system(s) are to be documented and managed, specifically: • unsupported hardware, software, and hosted services • evaluating the organisation's exposure to such vulnerabilities and taking appropriate measures to mitigate the identified risk(s). **Security requirements** Applications, products and services are often exposed to security vulnerabilities which may result in information being compromised. Security requirements provide a proper foundation of vetted security functionality for an application, product, or service. Organisations are to consider functional, non-functional and security requirements to ensure potential security risks are adequately managed by implementing the right set of mitigating controls. Identification of additional requirements could be performed as a result of risk assessments. Depending on the

Functional Process	Control Area	Requirement	Guidance
			purpose of the application, products or services, specific requirements such as the following may be introduced to maintain confidentiality, integrity, and availability of information: • information and asset classification including their dependencies and protection requirements • thorough testing of written code • access to written code restricted to authorised personnel only • encryption requirements for information while at rest and in transit • use of authorised and secure APIs • access to application and database is restricted to authorised personnel on a need-to-know basis only • additional security mechanisms such as MFA for privileged or administrator accounts • use of approved password managers • collection and retention of information only as required • use of logging and monitoring, data leakage prevention • documented and approved process of authorisation and approval • cyber security insurance in case of incidents • security testing. If any application is being developed or used for payments or financial transactions: • payment information from the payee is to be verified and protected • transactional information is not lost or duplicated, stored in a restricted environment, protected and retained in accordance with regulations • use of digital certificates and cryptography techniques.
Detect	Independent reviews	HML67: Independent security reviews are defined and implemented before any new or major upgrades on systems are moved to the production environment.	**Independent security review** Independent security reviews are to be performed against best practices on assets and procedures to determine whether the organisation has reasonable protection in place based on its risk profile. If these reviews are performed by an internal team, these personnel are to be independent from the rest of the organisation and not work for any other teams. These reviews are to be initiated by the organisation's Board or steering committee and by the project team for new systems and any major upgrades to existing systems within the organisation before they go live. **Security testing** A type of testing that uncovers vulnerabilities of the systems to determine that the information and its associated assets are protected from potential security threats. Security testing, or penetration testing, or vulnerability assessment can be used to either identify vulnerabilities or determine the ability of organisation systems to withstand attacks given various constraints (e.g., time, resources, and/or skills). Penetration testing mimics hostile cyber-attacks against the organisation and provides a more in-depth analysis of security-related weaknesses/deficiencies. Organisations may also use the results of vulnerability analyses to support penetration testing activities. Few organisations have multiple test environments that are used for various type of testing activities with various tools and technologies involved. Any new systems, upgrades, updates, new versions are to be securely tested in an environment that is similar to the production before rolling on to the production environment. This is to ensure

Functional Process	Control Area	Requirement	Guidance
			that the introduced system, product or service does not introduce vulnerabilities to the organisation's environment and that the tests are reliable by involving clinicians and non-clinicians as applicable or as needed. During these security reviews, configuration and code reviews as relevant, are also recommended to be performed. **Outsourced services** While outsourcing any of these services or developments, the organisation's documented and approved procurement procedures are to be followed. Contracts or agreements with suppliers need to set out security requirements, and services or products need to be evaluated before purchase. It is important that all production and non-production environments are monitored by the supplier for potential security vulnerabilities, adequate controls implemented along with managing access. In all cases, whether in-house or outsourced, scope, and purpose of the agreement for the testing has to be clearly defined and agreed upon before commencement to ensure no live or in-production assets are affected from potential incidents.

Functional Process	Control Area	Requirement	Guidance
Communications security Implementation of controls in this section ensures that the information that is being passed over networks, and its supporting information processing facilities is to be protected from compromise.			
Protect	Network security	HML54: Networks and network devices supporting the systems and applications are to be securely managed.	**Network security** Network security involves set of technologies, rules and configurations designed to protect the confidentiality, integrity and availability of information that is flowing in and out of an organisation's network. Tools are usually used to enable real-time network monitoring on endpoint devices and further strengthens the organisation's internal security. Moreover, when additional controls are being implemented, consider: • classification of information that is being passed within the network • identifying information, its associated assets, documentation and classification of all the network devices within the organisation's network • documenting management of all identified network devices along with diagrams, configurations, etc. Any changes to follow the organisation's documented change management procedures • backup or stand-by network devices are separated from the production environment • restricting access to the networks and network devices on a need-to-know basis • backup and restoration procedures for all operational network devices to maintain their integrity and availability • logging and monitoring activities • logs are being sent to central location for visibility, correlation of events, respond to incidents and overall management • as applicable, configure network devices such that content filtering is performed • restricting access to information systems via network devices such as firewalls and content filtering management software and hardware • hardening of network devices as per industry best practices • segregation between administrator and standard access to systems • rename or disable all default administrative accounts (e.g., root, administrator, etc). **Zero trust architecture** A zero-trust policy and zero trust architecture require personnel, applications and infrastructure to always be verified by using strong authentication methods across each application, segmented network and infrastructure components such as routers, switches, cloud, Internet of Things (IoT) and supply chain. The levels of authorisation required will vary depending on the business and security needs. Zero trust architecture focuses on each file, device, service, email, and network by authenticating each identity and device at all levels. It is also called "perimeter-less security". Policies such as conditional access, continually verify and evaluate identities and devices to ensure that access is provided at the right level to authorised personnel. **Virtual networks** To enable the communication between multiple computers, virtual machines, virtual servers, data centres, and other devices across different departments within the organisation, virtual networking is used. As administrators don't need to manually configure hardware, virtual networks can be set up more quickly in response to the organisation's requirements. This flexibility enables:

Functional Process	Control Area	Requirement	Guidance
			• faster service delivery • operational efficiency • improved network security and disaster recovery • faster network provisioning and configuration • improved control by allocating appropriate bandwidth for specific resources • specifying and enforcing security policies to meet auditing requirements. Virtual networks are desirable from a security viewpoint, since they can permit logical separation of communication taking place over physical networks, particularly for systems and applications that are implemented using distributed computing. A zero-trust network combined with network virtualisation provides the secure connectivity needed for endpoints to converse securely.
Protect	Segregation of networks	HML55: The systems and applications that are used to process, store, or transmit information are connected to a separate, dedicated network.	**Network segmentation and segregation** Network segmentation involves partitioning a network into smaller networks, while network segregation involves developing and enforcing a ruleset for controlling the communications between specific hosts and services. Network segregation isolates critical networks from external networks such as the internet, whereas network segmentation splits a larger network into smaller segments – also called subnets – usually through switches and routers. Technology teams can then create risk profiles and other appropriate security policies for user and device groups. Network segregation and network segmentation help to minimise the risks of ransomware, malware attacks and make it difficult for attackers to work their way laterally throughout the organisation's network even when they do succeed in gaining access. Implementation of network segmentation and segregation helps technology teams to improve productivity through enhanced alerting and auditing capabilities, which in turn provide critical insights into the overall network infrastructure. This helps the teams to be more efficient and agile in the organisation while enhancing digital transformation initiatives. Networks are usually segregated into domains based on levels of trust, criticality and sensitivity (e.g., public access domain, medical devices domain, legacy medical devices domain, wireless access for guests, wireless access for personnel, medical units), where connections to all wireless access are treated as external connections. While segregating the networks, their respective perimeters are to be well-defined to allow access to be controlled at a gateway level based on the security requirements, and criticality of information that is being processed at each segregated network domain. **Virtual local area network (VLAN)** A VLAN is a custom network which is created from one or more local area networks. It enables a group of devices available in multiple networks to be combined into one logical network that is administered like a physical LAN. The principles of separation and segregation apply to software defined networking (SDN), which are to be deployed in a secure manner by considering: • the principles of separation and segregation to the design and architecture of VLANs through access control lists (ACLs)

Functional Process	Control Area	Requirement	Guidance

			• VLAN trunking is not to be used on switches managing VLANs of differing security domains
			• administrative access is to be permitted only from trusted networks
			• unused ports on switches are to be disabled
			• MAC filtering is to be used as appropriate.
			
			Access to networks
			Rules are to be configured at the gateway level such that only authorised personnel and devices are connected to the organisational networks. If connecting from remote location e.g., working from home scenarios, implementation of remote access software allows users to connect to the organisational network over the internet in a secure manner. There are various ways to connect securely with the help of the following where access from unauthorised or untrusted networks are to be continuously monitored:
			• virtual private network (VPN): creates a secure tunnel between a personnel's remote computer and their organisational network. Setting up a VPN requires the user to either configure a server on their organisational network to run the VPN software or to enable VPN features on their organisational router. However, while implementing a VPN, consider:
			  • whether they have any known security issues
			  • whether the VPN supports MFA and other strong authentication controls
			  • what access and security logs can be configured and reviewed
			  • whether the VPN can support the organisation's security, operational and performance requirements
			  • whether the encryption level is at an acceptable risk to the organisation is documented in the risk register and monitored.
			• SaaS remote desktop tools: creates a connection between a personnel's device to a specific device within the organisation. While implementing this software, consider whether:
			  • the software is still supported and patched by the vendor
			  • the software supports MFA and other strong authentication controls
			  • audit (activity, access) and security event logs can be enabled and incorporated into the organisation's security information and event management (SIEM) for monitoring purposes
			  • the encryption level is an acceptable risk to the organisation is documented in the risk register and monitored
			  • conditional access policies can be applied to prevent logins from unknown devices or locations etc.

Functional Process	Control Area	Requirement	Guidance
Risk management Implementation of controls in this section ensures that the organisation continuously monitors, understands, controls, and manages cyber risks.			
Identify	Risk assessments	HML32: Risk assessments are performed on new and existing systems and applications that manage information to understand the risks posed to the organisation while using them.	**Security risk assessment (SRA)** A security risk assessment identifies information security vulnerabilities and evaluates how they might be addressed and prioritises them according to likelihood of vulnerabilities being exploited along with their impact. Performing an SRA helps the organisation to understand its business functions, operational processes, information systems, threat profile, threat landscape, risk profile and the information it needs to secure. An SRA is typically carried out by a Security Consultant, and often takes place when new IT services or infrastructure are introduced, or when a major change is made to existing services or infrastructure. Identifying and understanding the risks organisations face can help them: • assess and understand the organisation's ability to address the risk • understand whether the organisation is meeting its obligations to its patients, staff, partners and stakeholders • prioritise the work that needs to be done to prevent or mitigate a potential cyber security incident • manage the ongoing risks by understanding, assessing, and evaluating the current risks, controls and their effectiveness and the residual risks as a result of the assessment • to see if contractual and compliance requirements are met • close the security gaps and strategically develop the organisation's security program • reach an informed risk management strategy • agree on residual risk and any control non-compliance that may need to be addressed. • limit uncertainty on what may go wrong with organisational information systems • have better visibility of the information threat landscape. **Risk assessment methodology** Organisations may take a proactive and repetitive approach to address information security concerns. A documented risk assessment methodology or processes helps organisations to: • identify the threats, events and sources • assess the risks through likelihood and impact • identify and assess the severity of vulnerabilities • manage the identified risks • review the implemented controls for their effectiveness. **Risk assessment matrix** A risk assessment matrix, also known as a probability and severity matrix, is a tool used for risk evaluation. Depending on the likelihood and severity, risks are to be categorised as extreme, high, moderate/medium, or low/very low. As part of the risk management process, organisations use risk matrices to help them prioritise different risks and develop an appropriate mitigation strategy. While creating a risk matrix, consider: • identifying the risk profile – strategic, operational, legal, financial, reputational, and external • determining the risk criteria – likelihood, impact • assessing the risks – extreme, high, moderate or medium, low, very low

Functional Process	Control Area	Requirement	Guidance

			• prioritising the risks and implementing a mitigation strategy.
			
			Performing security risk assessments (SRA)
			A typical SRA is performed based on the criticality of the information and services which are being managed or processed by the application or service based on the results from the business impact analysis (BIA) as explained in the business continuity and disaster recovery domain. Organisations are to periodically carry out an SRA on new and existing systems and applications to understand their risk profile, or when any system changes are being introduced. Ideally, an SRA is to be carried out every two years. When carrying out an SRA, there is to be a representation from all departments where there are vulnerabilities., and an effective consultation and communication among all stakeholders.
			
			An SRA typically involves:
			• risk identification:
			  • identify potential threats, such as natural disasters, hardware failure, malicious behaviours i.e., performing threat modelling
			  • identify vulnerabilities including software, physical and human vulnerabilities i.e., performing a vulnerability assessment
			• risk analysis:
			  • analyse the implemented organisational and security controls, and determine the likelihood of the identified risks along with its consequence
			  • determine the controls (deterrent, preventative, detective and corrective) to mitigate or manage the risk
			  • document the results to develop a risk assessment report which is to be acknowledged by the business owner (and risk owner unless they are not the same personnel)
			• risk evaluation: evaluate the risks against the organisation's tolerance levels i.e., risk profile
			• risk treatment: select, implement and evaluate the effectiveness of controls which modifies the risk status (accept, treat, avoid, transfer) of the documented risks in the risk register
			• risk treatment plan or security risk management plan (SRMP): once the treatment for the risks is selected, it is the process of implementing those treatments which includes the implementation details of action plans as documented and approved. This could be applicable to individual systems or applications processing or storing information or a single plan for the organisation covering all information processing systems or applications
			• system security plan (SSP): contains details of system description, system boundary, architecture, and security controls in one document along with the details on how all the security controls are implemented
			• monitoring and review: continual assessment of risks to ensure that the selected treatment remains effective. This ensures that likelihood has not increased and to ascertain if the cost of the control(s) to reduce the impact has decreased to a level that makes its implementation affordable
			• communication and consultation: effective communication between stakeholders is to ensure that risks are understood and decisions about risk response selection are appropriate.
			
			While performing a risk assessment, risks associated with both internal and externally hosted systems, applications and services are to be considered along with ICT supply chain risks. ICT supply chain risks are managed through the procurement process, technical checks and control assessments.

Functional Process	Control Area	Requirement	Guidance
			Any changes which are being performed to the service or system or application as a result of risk assessment process is to follow the organisation's documented change management procedures. **Risk register** A risk register records all of organisation's identified risks and the decision(s) taken by management against each. A simple, consistent format makes it for relevant personnel to understand the information as it also contains the likelihood and consequence of a threat occurring, actions along with the timelines undertaking to reduce the risk, personnel responsible for managing them in one, easily accessible location. It is also important to document the management decision with regards to addressing the risk. While documenting the risks within the risk register, consider: • documenting the risk description including the cause and the outcome (impact on patient, operational, financial, and contractual perspectives) • status of the risk (open / closed / accepted / avoided) • security controls or measures that are already in place, the one's that needed to be implemented and their effectiveness • risk or business owner to each identified risk • date raised • determine the current threat likelihood and impact of the risk materialising and the accumulative risk level i.e., current risk rating • identifying existing controls to reduce, mitigate, transfer, share or avoid the risk • estimating the residual risk likelihood and impact of the risk materialising, and risk level i.e., residual risk rating • date of next review. **Threat and vulnerability assessment (TVA)** To identify consequences and risks as part of an SRA, a threat and vulnerability assessment is conducted to categorise both malicious and non-malicious threats, and vulnerabilities. The impacts of these risks would fall under various categories as defined in threat landscape as they may impact confidentiality, integrity, availability of information. TVAs take different forms, including scenario-based network, penetration testing, web application testing, social engineering testing, wireless testing, configuration reviews of applications, relying servers and databases along with detection and response capability evaluation based on the sensitivity of the information which the application or services handle. **Penetration testing** Sometimes referred to as a 'pen test' or 'ethical hacking', penetration testing simulates a cyberattack to identify vulnerabilities in a system or application. This helps developers correct the identified vulnerabilities before potential exploitation by hackers or attackers or malicious users and other threat actors. Organisations are recommended to schedule regular penetration testing, and also carry out this testing whenever a new component or system is introduced or an existing one is upgraded to protect confidentiality, integrity and availability of information. **Control catalogue**

Functional Process	Control Area	Requirement	Guidance
			This is a collection of all security and privacy controls that are required to address risks in the risk register. The controls will be prioritised in order of importance but each one is needed to ensure information is secure. A unique identifier is assigned to each control which contains its description describing the behaviour, mechanisms or indications of implementation along with its priority. Regardless of priority of the control, all controls need to be implemented to achieve adequate security for information. **Controls validation plan (CVP)** The CVP outlines the approach or scope of the CVA. This specifies the controls to be audited and how their effectiveness will be assessed, through workshops, interviews, observations, document reviews or configuration reviews. **Controls validation audit (CVA)** The purpose of the CVA is to verify whether the controls recommended in the risk assessment have been configured, implemented, and are operating effectively to ascertain the current status of the identified risk.

Functional Process	Control Area	Requirement	Guidance
Operations security Implementation of controls in this section ensures that: • a copy of information is available if it is lost, leaked or stolen i.e., information backups • changes to information, relevant processes, processing facilities, and systems follow a formal and structured change control process i.e., change management • exploitation of vulnerabilities is prevented, and integrity of operating systems is being maintained i.e., patch management • the information systems and its associated assets are securely configured i.e., configuration management • the organisation identifies gaps or issues that requires resources to address i.e., capacity management • the information and its associated assets are protected from malware i.e., endpoint security • information is not disclosed to unauthorised individuals i.e., data leak prevention • the activities that are being performed on information is appropriately logged and monitored i.e., logging and monitoring			
Information backups			
Plan	Policies and procedures	HML17: A backup and recovery procedure is in place.	**Backup and recovery procedure** Organisations are to establish their own procedures for backing up and recovering information. These procedures define roles and responsibilities, schedules for performing backups and respective restorations. It also includes the measures which will be taken to recover from a disaster and who has access to these backups. While developing backup and recovery procedures, organisations are to consider: • identification of critical information, systems, its associated assets • types of backups that will be scheduled (full, differential, incremental) • frequency of backups and restorations based on the criticality levels • recovery point objective (RPO) and recovery time objective (RTO) as identified in business continuity and disaster recovery plans • how backups and archives will be encrypted • how backups will be stored i.e., online and protected from ransomware attacks, off-site and stored in a fireproof safe • roles and responsibilities of backup administrator • information backup and restoration retention requirements • offsite rotation requirements • procedures and requirements to be followed for backup and restoration • how retentions requests will be processed • security requirements when restoration is required • backup and restoration retention requirements • loss of data response procedures • process for non-electronic off-site data storage (e.g., tapes) • testing of backups/restoration. These documented procedures are to be periodically reviewed and approved by authorised personnel before being communicated to relevant parties. Any changes identified are to follow the organisation's change management procedures. Exceptions identified are to have a valid business reason, approved and documented for reference.

Functional Process	Control Area	Requirement	Guidance
Protect	Information backup	HML56: Backup copies of information, software and relevant systems are protected and maintained in accordance with the backup and recovery procedures.	**Backups and recovery** Organisations use information to make informed decisions to offer personalised services to their patients. Information backup and recovery are practices of building and storing copies of information to protect organisations against data loss and to ensure its future availability and integrity. Backup and recovery of information and relevant services are essential for enhancing cyber security, minimise downtimes and to reduce costs in times of crisis. Some cloud-based tools offer backup and recovery services along with the ability to tailor the storage needs of organisations based on the volume of their information. As data theft or loss can have a direct impact on patient care, data backup and recovery are essential parts of any organisation's technology strategy. If the organisation chooses to implement a cloud-based solution, data sovereignty, jurisdictional and legal boundaries are to be considered. Ideally, there are to be three copies of backups for information, stored in at least two locations, one of which is a remote location. Depending on the criticality of the information, its associated assets, and services, backups may be incremental, differential or full. This is to ensure that information and relevant services can be recovered following an incident or failure or loss of storage media. **Backup and recovery plans** A backup and recovery plan provides details on what information, services, its associated assets need to be backed up, frequency of backup, its restoration procedures, frequency of restoration, archival of backed up and restored information. Some information may need backing up relatively infrequently. By contrast, critical information like patient information might need multiple daily scheduled backups. Also, a backup and recovery plans for information and its associated assets will require: • successful and complete backups are carried out following documented procedures • backups are carried out according to the information's criticality and recovery point objective (RPO) requirements • if not using cloud backups, backup copies are securely stored in an offsite location and is accessible by authorised personnel only • backups stored offsite are protected with appropriate physical and environmental controls with similar level of standards applied at the primary site • backups are encrypted to protect their confidentiality and integrity • clear steps on backup and restoration of information • the information is able to be recovered within the agreed recovery time objective (RTO) and recovery point objective (RPO) requirements. **Backup storage** It is critical to store backup information on a separate source to protect against data loss or corruption. To keep backup information safe, it is recommended to: • follow the 3-2-1 rule (3 copies, two locations, one of which is off-site) • increase frequency of backups • align backup strategy to service level agreements • perform cloud backups with considerations to data sovereignty and jurisdictional boundaries • automate disaster recovery • data retention is to be kept in a separate dedicated storage environment to where production or backup data is.

Functional Process	Control Area	Requirement	Guidance
			Backup retention After information has been backed up, it needs to be retained in case of an unplanned event or incident. Exactly how the information is to be retained will vary but typically, a retention procedure is to consider: • how long the information is to be retained for • how the information is to be retained • what information is to be retained and why • when to dispose the retained information • having the latest full copy of the dataset in case the plan is to only take incremental backup datasets which may not be kept for a long time • retaining at least the last three copies of a backup. The information which is backed up is to be retained so that the retained backup copies allow information to be restored from an earlier point in time for organisations to recover in case of an unplanned event or a cyber incident. It is important to store the retained information at a different compatible source to protect against data loss or corruption. It is important to consider contractual, legal, regulatory, statutory, and security requirements while retaining information to maintain its compliance. Information retention is usually performed based on the: • type of information and its segregated security requirements • information lifecycle • number of type of versions which are to be stored • types of backups and their frequency.
Protect	Backup restoration	HML57: Backups are tested for their restoration in accordance with the documented backup and recovery procedures. Organisations are able to access restored backups as well.	**Backup restoration** Restoration of the information which is already backed up helps organisations to recover from unplanned events, makes a usable copy of information available to replace lost or corrupted information. It is important to periodically test the organisation's backup and recovery plans to ensure that information is not being corrupted or lost during the process. During restoration, consider: • recovery point objective (RPO) – or the amount of data loss the organisation considers acceptable in an emergency • recovery time objective (RTO) – or the organisation's target for how long it takes to get back up and running after a loss • security of the information during and after its restoration activities • zero impact on the performance of the organisation's technology operational procedures. If the documented processes are not meeting any of the above, the processes are to be fine-tuned such that the metrics are achieved. Any changes which are being performed are to follow the organisation's documented change management procedures for reference purposes. Ideally, backup restorations are to be tested every quarter, and measures taken to avoid accidentally overwriting production information. Due to a variety of services and systems being used, it is imperative that not one restoration process covers all services and systems. It is recommended that all critical services and systems are to be considered every quarter for testing backup restoration processes against the objectives of incident response and the documented business continuity plans in the case of a disaster.

Functional Process	Control Area	Requirement	Guidance
Detect	Monitoring of backups	HML68: Authorised personnel or teams are alerted upon unsuccessful or incomplete backups.	**Monitoring** It is important to monitor backups to identify any potential issues so that they are dealt as soon as possible and are resolved efficiently. Backup monitoring tools automate the alerting process on failed on unsuccessful backups to backup or IT administrators to ensure that they are rerun or rescheduled promptly. These tools can also help indicate trends, such as backups which are regularly unsuccessful. In turn, this helps administrators finetune the backup process as required, following the change management process. If any changes are being performed on the schedules of backups, the organisation's documented change management procedures are to be followed. Logs of backup activities along with their schedules are to be monitored for potential security incidents via a centralised platform wherever possible. If a platform is not available, logs are to be reviewed daily for critical systems and at least once a month for non-critical systems.
Change management			
Plan	Policies and procedures	HML18: A documented process is in place for performing changes to new and existing systems or services related to information.	**Change management process** Change management is an organised, formal, and structured approach with processes or mechanisms that enable organisations to transform workflows. This also helps in reducing potential business and security risks to the organisations. Changes are performed when personnel, processes, teams, and tools cannot keep up with the needs and expectations of the organisation's business, security goals and objectives. This helps to ensure confidentiality, integrity and availability of information. There is a need to build focused and structured change management plans to guide personnel to achieve required major or minor outcomes. An effective change management process includes: • scope of the process • change advisory board (CAB): the group of personnel who assess, prioritise, authorise, and schedule changes. A change manager is usually responsible for organising these meetings (recommended weekly). The CAB is usually made up of representatives from different parts of the organisation, such as technology, security, operations, and other business units • change request management: structured way of handling changes that are submitted to the change manager (for normal and emergency changes) to initiate, record, assess, approve/reject and resolve changes • change management log: a list of formally managed changes that are being tracked for progress from submission through review, approval, implementation and closure • change categorisation: changes are grouped and categorised based on the level of impact and urgency, ranging from planned major changes (results in business disruption during regular hours), to normal or maintenance or minor changes (e.g., operating system hotfixes or regular patch cycles), to emergency or unplanned changes (e.g., a response to outages, business continuity). The change management process is to be reviewed along with other policies and processes within the organisation at least annually, or whenever there are applicable changes made within the organisation. The change manager will need to analyse the number of standard or normal and emergency changes to ascertain if the volume of emergency changes is higher. It is also recommended to audit the changes that are performed on information systems. This helps organisations in managing their changes effectively by: • assessing the current state of the process

Functional Process	Control Area	Requirement	Guidance
			• identifying the gaps • document and track modifications to the process • implement the modifications • monitor and evaluate the process. For any changes which are being performed within the organisation especially, if they are affecting the patient health care, testing is to be performed on a test system (as applicable) prior to rolling them out to the production system. Mechanisms are to be in place to identify incorrect changes which are performed. **Change management document** All changes which are being performed within the organisation are to be documented and updated throughout the change management process. An effective change management document is to include: • purpose and scope of the change • business owner and change owner approvals • areas that will be affected (process, technologies, personnel or teams) • classification of the change • how the change can be rolled back, if necessary • how the change will be tested • how the change will be communicated • when the change will be made • who has approved the change. Once a change is performed, relevant documentation may need to be updated, including operating procedures, continuity plans and recovery plans. **Change management communication** Effective communication is an important part of any change process. Stakeholders are to be informed about what is happening and why, and how the change might affect them. The communications required will vary depending on the specific changes being made. For standard planned changes like regular patch updates, the communications required might be relatively minimal. For a major change or for one that is unexpected and is affecting normal work routines i.e., an unplanned outage, more details and regular updates may be required. **Unauthorised changes** Changes which are implemented without all relevant approvals are often categorised as unauthorised changes. Unauthorised changes are to be reported to the change manager, who may: • roll back the performed changes • update the change management log • submit a new change request to reflect the performed changes. Once identified, these unauthorised changes are to be raised as potential security incidents and investigated immediately for potential compromise of information.

Functional Process	Control Area	Requirement	Guidance
			Emergency or unplanned changes These changes are those that need to be made to resolve major incidents which may pose severe risks to organisations. Because of their urgency, these changes do not follow regular change management processes, and may need to be implemented outside the normal change window. As soon as an emergency change is raised, the change manager brings it to the notice of available CAB members for a decision. Where delays in changes could result in high costs, it is also important to note that retrospective documentation is to be completed to keep track of the changes which are being performed and is communicated to respective stakeholders. **Auditing changes** Changes that are being performed on information, its associated assets along with the process followed is to be periodically reviewed by: • assessing the current state of the process • identifying the gaps • documenting and tracking modifications to the process • implementing the agreed or approved modifications • monitor and evaluate the process for assurance.
Identify	Security testing	HML33: The proposed changes are to be analysed for potential security threats and their impact on the organisation.	**Change impact assessments** When changes are proposed, a change impact assessment is to be performed by the change or business owner to predict and anticipate the impact of the change. These assessments help the decision makers or the CAB to decide on the proposed changes. **Penetration testing** Sometimes referred to as a 'pen test' or 'ethical hacking', penetration testing simulates a cyberattack to identify vulnerabilities in a system or application. This helps developers correct the identified vulnerabilities before potential exploitation by hackers or attackers or malicious users and other threat actors. The types of penetration testing which are to be performed will vary depending on the changes being performed. Vulnerability assessments are performed to identify the existing known or potential weaknesses, vulnerabilities within the organisation environment. Organisations are recommended to schedule regular penetration testing, vulnerability assessment, and also carry out this testing whenever a new component or system is introduced or an existing one is upgraded to protect confidentiality, integrity and availability of information. Any risks identified during these assessments are to be recorded in the organisation's risk register, and controls put in place to manage or mitigate the risk.
Protect	Separate production and non-production environments	HML58: Organisations developing inhouse systems, applications or services are to maintain separate	**Separate environments** Separate production and non-production (development, test, etc) environments prevents developers from accidentally modifying or deleting information while developing new or enhancing existing systems or applications or services. Working with multiple environments and following a deployment process helps in streamlining the

Functional Process	Control Area	Requirement	Guidance
		production and non-production environments.	workflows and reduces the potential for errors. In all cases, information is to be protected against tampering, information disclosure, spoofing, non-repudiation, and loss, especially when anonymised health records are being used between different environments. **Development environment** This is a workspace for developers to make changes without affecting the live or production environment. Any identified issues or errors are initially dealt with in this environment for further testing. **Test environment** A separate environment is to be used for testing purposes to understand if the required objectives are met and to avoid interrupting services or applications affecting information. Information (if personally identifiable) is to be anonymised when being used in the test environments and is to be kept separate from production data. It is recommended to perform an additional review while anonymised data is being used for testing purposes. **Staging environment** A staging environment is where final testing is carried out before a system or application is deployed to production. Each staging environment is to mirror an actual production environment as accurately as possible, including all safety and security measures. **Production environment** A production environment is where the system or application is deployed for organisation personnel to use. When using multiple environments, it is important to consider: • access privileges for the different environments are based on roles and responsibilities such that segregation of duties is maintained after prior approvals • production and non-production environments are to have separate domains, and appropriate authentication procedures • testing is to be carried out in the non-production environment only, unless a formal change request to the contrary has been approved • production and non-production environments are clearly identified • all environments (including tools that are being used) are to be updated with the latest security patches as per the organisation's documented patch management policy or process • applications and systems are to be securely configured • any changes being performed are to follow documented change management processes • activities on all environments are to be logged and monitored for potential security incidents, and regular backups and testing are to be performed. In some cases (e.g., cloud applications), there might not be separate environments and changes are rolled over from one instance to the other. To reduce the downtime while performing any changes, high availability is to be considered at an architectural level.

Functional Process	Control Area	Requirement	Guidance
Patch and vulnerability management			
Plan	Policies and procedures	HML19: A documented process is in place for identifying vulnerabilities and updating patches on the organisation's systems, applications, tools, services etc.	**Patch management** Both software and hardware are to be kept up to date ("patched") on devices (including printers) where information is stored, processed or transmitted. Responsibility for patch management lies with the technology teams, who are to receive regular notifications on the latest patch releases. The releases are then validated to see whether they are fit for purpose, and they are deployed following the organisation's change management process. **Vulnerability management** Vulnerability management is a set of continuous monitoring processes designed to secure organisation networks and devices against potential cyber-attacks. These practices provide an overview of an organisation's security posture and the areas that are at most risk, in order to prioritise security remediations. Vulnerability scanning tools are to be used whenever possible to identify vulnerabilities and determine when they are resolved. **Patch and vulnerability management process** Patch and vulnerability management are the first line of defence to remediate vulnerabilities. The documented process sets out the requirements to manage information security vulnerabilities, along with notification, testing, and installation of patches. For management of vulnerabilities, consider: • frequency of vulnerability scanning (manual or automatic) based on business and security requirements. In some cases, scanning may be a continuous process while in others it may be done whenever a change is made or on a fixed schedule (e.g., annually). • issues identified during scanning are to be evaluated, prioritised, tested and mitigated • responsible roles for performing scanning. This will typically be system, service, application or product owners • how suppliers communicate with organisations when vulnerabilities are identified and how they can be contained. For management of patches, consider: • an appropriate risk informed patch cycle for all operating systems, and timeframes deploying emergency patching (typically within 48 hours of the release) • expectations around maintaining systems, services, or applications with current OS, application, or security patch levels, as recommended by the software manufacturer and informed by the risk owner • verifying that the patches are released by authorised sources only • testing and approval of patches before being rolled out into a production environment • as necessary, rolling back unstable patches • authorised roles to deploy patches. For management of both patches and vulnerabilities, consider: • RASCI matrix for maintenance of patches and tracking vulnerabilities are to be determined, reviewed and updated based on the roles and responsibilities within the organisations • identified vulnerabilities along with patch updates are to be measured and reported to the organisation Board

Functional Process	Control Area	Requirement	Guidance
			• any deviations from the patch cycle or actions taken to address a known vulnerability are to be approved by authorised personnel; the risks are to be updated in the risk register and compensating controls are implemented to manage the risk • auto updates are enforced wherever possible to minimise the chance of human error. The documented process is to be reviewed along with the other organisation policies and processes, or when there is a security incident as a result of issues identified in the process. **Other procedures** As well as having a patch and vulnerability management process, there could be other standard procedures to support the process are to include: • detecting of the existing vulnerabilities in all the systems, services and applications which are being used within the organisation • an effective and efficient way to communicate as soon as vulnerabilities are identified and involve necessary teams to analyse and remediate the vulnerability • identifying the risks associated with the identified vulnerability along with the mitigation measures to be taken • testing the patches on testing and/or staging environments before rolling them into production environments by following documented and approved change management procedures • the latest stable version of the software or the patch is to be installed subject to the risks identified are documented, managed and approved by the management • roll back procedures are tested and implemented if the updated patches were unstable • patch updates are obtained from authorised sources only • only authorised personnel and/or automated authorised service accounts are to perform patch updates and scan the organisation's environment for potential vulnerabilities. The documented patch and vulnerability management process usually works in conjunction with the organisation's incident management process. This allows the incident response team to respond effectively to the potential incidents which could be raised. If any of these activities are outsourced, organisations are to obtain service reports from the suppliers to understand the status of their technical environment.
Protect	Patch and vulnerabilities remediation	HML59: Identified vulnerabilities or unpatched systems, services or applications within the organisation are properly identified, tracked and remediated.	**Unpatched software or known vulnerabilities** Unpatched or vulnerable software can be exploited by cybercriminals. If there is a patch available, it needs to be implemented immediately and if there is a known vulnerability which does not have an available patch, it is to be reported immediately to the manufacturer or service provider. Vulnerabilities and unpatched software are to be tracked in the organisation's risk register, monitored and managed until they are resolved. Risks are usually managed by: • implementing workarounds and/or mitigation strategies as suggested by suppliers or other authorised sources (after having them approved and authorised by the business owners) • disabling the vulnerable services (if the risk cannot be accepted) • setting up additional firewall rules to restrict the traffic

Functional Process	Control Area	Requirement	Guidance
			• putting additional monitoring in place to prevent unauthorised access to information • enforcing conditional access policies to limit access. If organisations use vulnerability scanning tools, it is important to make sure that these tools are also updated with vulnerability signatures and security patches before performing any scans. This ensures that the tool(s) do not violate organisation policies by leaking information or exposing information to unauthorised parties due to a vulnerability within the tools themselves. **Logging and monitoring** The activities of updating patches or performing scans are to be logged for investigation purposes to address potential cyber security events. This also helps in determining if vulnerabilities are exploited either intentionally (due to insider threat) or accidentally. These logs are to be correlated to a centralised logging system where possible with alerting mechanisms in place. **Cloud services** Where an organisation uses cloud services, it is the responsibility of the cloud service provider to manage the vulnerabilities. The cloud service agreement is to set out various parties' responsibilities, processes for reporting potential vulnerabilities, and how vulnerabilities are to be resolved. If there are shared responsibilities between the cloud service provider and the organisation, procedures are to be documented such that the potential or identified vulnerabilities are mitigated and managed.
Configuration management			
Protect	Secure configuration	HML60: Organisations have a standardised baseline configuration in place for new and existing systems, services and applications.	**Configuration management** For continuous patient care, organisations will need to have robust, secure and stable systems that support the information. Configuration management applies to a variety of information systems such as servers, operating systems, networking systems, applications, software, databases, cloud-related services and other storage systems. For systems and services used to manage information, an established configuration management process maintains consistency and their desired state. The advantages of this process include: • automatically manage and monitor updates to configuration data • act as the "source of truth" with a central location for configuration to help avoid discrepancies • version control (i.e., better visibility to configuration modifications, rollback functionality, consistency across all deployments, etc) • reduced risk of potential intentional or unintentional security incidents • unnecessary duplication of technology • improved user experience for clinical and non-clinical staff • restoring services more quickly if any problems occur • identifying all code and configuration deployed into the production environment • allowing creation of a duplicate or sandbox environment for any bug fixes • ensuring system configurations are protected from unauthorised or incorrect changes.

Functional Process	Control Area	Requirement	Guidance
			Automation tools are often used to maintain configurations based on the needs of the organisation. When selecting an automation tool, it is important to consider its performance, scalability, compatibility with existing systems, ease of use, support and security. Change management and configuration management often go together but it is important for organisations to understand their differences and use them where appropriate. **Baseline configurations** A baseline configuration is a documented, formally agreed set of specifications for information systems. Any additional requirements or changes to these configurations are to follow documented organisation's change management processes. In case of potential incidents, it is easy to identify if any information asset is not configured properly which may lead to a security vulnerability. During the investigation of a security incident, a baseline configuration provides a snapshot of the status of things which helps in comparing the status of the assets with their baselines. These baseline configurations are to be reviewed at least once a year against industry best practices. Any deviations identified are to be tracked in exception register and the one's that cannot be fixed are to be recorded in the risk register for mitigation or management. **System hardening** Securing a server or computer within the organisation with the help of tools, techniques and best practices to minimise potential cyber-attacks is known as system hardening. This limits the points of entry into the organisation environment by a malicious user and possibly reduce the number of points that can be targeted for attacks. For the same reason, approved and licensed software and tools are to be used within organisations to process, store or transmit information. If any unauthorised software is identified (i.e., shadow IT), the impact of not using the software is to be determined and the identified risks are documented within the risk register and managed. **Open-source software** Open-source software is often used when developing systems or services for organisations. When using open-source software, it is important to: • restrict access to authorised personnel • only use the latest and most appropriate releases of the software • log and monitor all activities to allow potential security incidents to be investigated. Open-source software needs to be regularly monitored for potential vulnerabilities, and patches implemented when available. If no patches are available or the software is not being maintained, mitigation strategies need to be put in place, and risks recorded in the risk register and monitored.

Functional Process	Control Area	Requirement	Guidance
Capacity management			
Protect	Capacity management	HML61: The capacity requirements for maintenance of information processing facilities, communication and environmental support during contingency operations are met.	**Capacity management** Organisations processing and storing information will need resources to maintain respective technologies based on their criticality at the right time, in a cost-effective manner. These resources are to be monitored and tuned based on the defined requirements such that the required systems, applications or services meet their performance requirements (in case of a patient surge). High availability, load balancing concepts and monitoring tools are often used to manage the capacities of systems within the organisation for tuning purposes. Identified additional resources are procured as required based on the importance of maintaining information on specific systems, services or applications. It is the responsibility of the system owners to manage this along with the inputs from monitoring or relevant teams. Internal teams are to provide a report to respective system owners on the available capacities so that budget allocations can be made for additional purchases. If managing capacity is outsourced, organisations are to include this as part of regular service reports for consideration and action. While increasing capacity, consider: • hiring new personnel to perform the activities as required if there is no skillset available within the organisation • obtaining additional storage or physical space if required to add additional devices • preference to be provided for usage of cloud computing mechanisms where possible • fine tune existing backup requirements if additional storage is being added • decommissioning of the systems or applications which are not being used to free up existing resources • current availability requirement of business-critical functions, applications, processes and considerations for better resilience • sudden spike in utilisation of resources beyond their normal or set threshold automatically alerts the administrator and relevant system owner • estimating benchmarks for future projects using past analysis and fresh assessment of current capacity and demands.
Endpoint security			
Protect	Malware protection	HML62: Information, services, and applications on organisation systems and associated assets are protected against malware.	**Malware** Malware or malicious software is a code or a file that is designed to cause disruption to networks, services applications or operating systems to gain unauthorised access to systems or information. There are multiple types of malware such as adware, botnets, cryptojacking, malvertising, polymorphic malware, ransomware, remote administrator tools (RATs), rootkits, spyware, trojans, virus and worm malware. Malware may be introduced into systems in the form of email attachments which contain malicious code, via file servers, file sharing software, or through remotely exploitable system vulnerabilities. **Protection against malware** There are various tools that can be used to detect and prevent malware, including firewalls, intrusion prevention systems (IPS), endpoint detection and response (EDR) agents, threat management systems, anti-virus software, and content filtering on web applications. Malware detection software is to be regularly updated to ensure

Functional Process	Control Area	Requirement	Guidance
			signatures are up to date. Alongside implementing tools and software, there are a number of processes and strategies that can help block malware such as: • implementing software rules to prevent the use of unauthorised software, or to block suspicious websites • implementing anti-malware rules to block any suspected viruses • testing regularly to identify any vulnerabilities on critical systems and applications • updating operating systems with the latest patches • following documented change management processes to make any changes to critical systems and applications • following approved and documented procedures while providing access to information, and associated assets • scanning files and other attachments for viruses received from other entities either in the form of emails, external storage or file sharing mechanisms before opening them. • developing recovery plans for information in case of malware infections • implementing warning banners to notify personnel of potential malicious websites • developing detection and response capabilities along with playbooks to handle potential incidents • training personnel about the risk of malware when opening suspicious emails, downloading software, and while accessing websites. Any systems or devices infected with malware are to be treated as a potential incident and follow documented incident management procedures.
Data leakage prevention			
Protect	Data leakage prevention	HML69: Organisations are to detect and prevent data leakage through the unauthorised disclosure and siphoning of information by individuals, systems or services.	**Data leakage prevention** The process or practise of detecting and preventing the loss, leakage and misuse of information from unauthorised access, etc is data leak prevention. This makes sure that personnel send only the relevant information within and outside of the organisation network. **Tools and technologies** Data loss prevention (DLP) technologies have become essential to protect information, particularly as more information is stored in the cloud-based SaaS applications. These technologies help to protect information when it is being used, stored or transmitted. In general, advanced tools and technologies are deployed to help monitor, detect, and block information from being transferred out of the organisation network. This would further prevent personnel from saving local copies of information, transferring it into external media, etc and deny their permissions if such actions are being performed, unless an exception was already provided. In addition to these tools, the implemented tools and technologies can also monitor incoming emails for malicious attachments or suspicious links. In certain cases, information may need to be shared outside the organisation's network. In these cases: • approval needs to be sought and documented • only authorised personnel are to share information over an encrypted channel with other authorised personnel who have similar clearance levels

Functional Process	Control Area	Requirement	Guidance
			• while specific roles are authorised to copy or export information to share outside of the organisation's network, data owners are to approve the copy or export of the information. However, the onus lies on the personnel within those authorised roles in the event of an unauthorised data leakage • restrict taking screenshots or photographs of the screen or screenshare or screen recording using third party tools and technologies. This is usually covered via an acceptable use policy or user training and awareness programmes. **Implementing DLP** When implementing data leakage prevention technology, the following issues are to be considered: • network: the solutions implemented provides a greater visibility of the activities on the organisation network which allows the monitoring and management of the flow of information via the organisation's network, internet or email • endpoint: the solutions implemented monitor endpoint devices, such as servers, computers, laptops and mobile devices, on which information is used, transmitted, and stored • cloud: the solutions implemented protect the information stored in the cloud by encrypting sensitive information following a specific standard and ensuring that the information is sent to only those cloud applications that are authorised by the organisation. The organisation is to consider the following to reduce the risk of data leakage: • classification of information and enforcing the access rules based on the classification • monitoring email, file transfers, mobile devices, portable storage devices, etc • precautionary measures which are to be enforced via policies, procedures and awareness training to prevent leakage of information.
Logging and monitoring			
Detect	Logging and monitoring	HML70: The activities performed on the information processing systems, services and applications are logged and stored as per the organisation's logging and auditing requirements.	**Logging and auditing** Recording the occurrence of an event at the time it occurred, performed by the responsible personnel or service and the impacted system or service is known as logging. This could include any hardware, software, or implemented controls to track activities such as modifying information assets including protected information within information systems and the services that are dependent on them. Many hardware devices and software can audit and log various activities, including network traffic, internet access, creating or deleting users, adding users to groups, changing file permissions, transferring files, opening a sensitive record, powering off, deleting or tampering with system logs, and anything else a user, administrator, or the system itself might do. Auditing, on the other hand is the process of evaluating these recorded logs and corelating events against an agreed benchmark of what normal looks like and report findings and/or deviations if any occurred. **Logging and auditing requirements** Auditing and logging are first line of defence and essential for systems and services which are used for processing or storing or transmitting information, relevant services and troubleshooting if any problems arise. A framework is to be established to monitor and review the logs which are generated from various sources such that any potential events related to security can be handled appropriately. This framework is to consider:

Functional Process	Control Area	Requirement	Guidance
			• technical control implementations, or processes for logging, identification and continuous monitoring of access, changes, command execution to all information assets • monitoring practices that are tailored to the criticality of the infrastructure, data, and applications alongside regulatory and legal expectations around monitoring • enabling audit logging to record the date, time, authentication activity with a unique user and system identifiers including all failure or change actions. Audit logging is also to include commands issued and relevant output generated to provide enough information to permit reconstruction of incidents and move system(s) to its original state in case of incidents • encrypting all logs while they are in transit or at rest. **Recording an event** Unauthorised access to information and its associated assets is to be recorded and monitored for potential security incidents and documented incident management procedures followed. However, while recording the events, organisations are to consider: • category details – application, database, security, setup, system • date and time of the event • description or information of the event • warning or severity of the event • identifier for the event • event success or failure security log • other information such as IP addresses, hostname or username or device **Log analysis** Logs are to be aggregated, correlated, reviewed and analysed periodically for potential incidents that might have compromised information. It is important to have a clearly defined and documented procedure for this analysis. When analysing logs: • only authorised personnel with necessary skills are to access the logs and perform the analysis • exceptions identified through the use of pre-defined rules are considered and pre-documented • user and entity behaviour are considered • correlate logs with other sources or flow of information. **Collection and storage of logs** To maintain the performance and security of an organisation's network, it is essential to collect and store logs from various information sources. The collected logs are to be reviewed regularly based on the security objectives and compliance requirements of the organisation. This helps to uncover misuse of patient information or information processing systems. Audit logs are to be stored as per the organisation's data retention policy. While storing audit logs, consider: • any contractual or legislative requirements • ability to extract the logs in a readable format for e-discovery or other purposes • that they cannot be altered in any way. Alerts are to be generated if changes are performed and documented incident management processes are followed • limit viewing of audit trails to specific roles based on their job requirements • backing-up audit trails to a centralised log server or media that is difficult to alter in a readable format

Functional Process	Control Area	Requirement	Guidance
			• reporting the audit logs which are on/off at any point in time • transferring logs centrally through encrypted mechanisms separate systems (e.g., SIEM solution) which are not the same as the source systems • if applicable enforce biometric authentication or any other alternative to access logs to protect against repudiation • abnormalities identified are to be handled as per the documented incident management process. If this functionality is outsourced, agreements are to ensure that the contracted organisation will support the organisation with reviews and investigation of potential security incidents. **Real-time monitoring** Various tools are used for monitoring (continuous or performed at regular intervals). Due to the types of attacks, the tools are to be flexible such that the threat landscapes can be adopted, and the teams are alerted based on pre-defined thresholds or incident response playbooks. Alternatively, alerting tools such as antivirus, intrusion detection system (IDS), intrusion prevention system (IPS), web filters, firewalls, data leakage prevention are to be used to provide real-time alerting when a log processing failure occurs or if an inappropriate access or change is identified. If any abnormal events are identified, they are to be logged as potential incidents and documented incident management processes are to be followed. **Security information and event management (SIEM)** SIEM solutions combine security information management and security event management into one security management system. These solutions offer a wide range of capabilities from log management, to event correlation and lastly incident monitoring and response capability. While collecting, monitoring and analysing events, it is crucial for organisations to manage the security of information by filtering and prioritising the alerts which are generated by the software to respond to potential security threats and vulnerabilities before the organisation's operations are affected. SIEM tools: • usually integrate with common vulnerabilities and exposure (CVEs), and latest signature databases to ensure that systems are evaluated and monitored against known vulnerabilities • are also used to collect logs and manage them from various applications, systems, databases, network devices etc under one umbrella • reduction in noise and false positives and negatives provides the ability to perform targeted investigations which improves triaging and the overall incident response capability • come with dashboards that can offer visibility into the organisation's activities within their network so they can respond swiftly to potential incidents and meet legal, contractual, and regulatory requirements • limit phishing attempts, provide IP rule blocking and user deprovisioning • can generate reports for audit and compliance requirements.

Functional Process	Control Area	Requirement	Guidance
Detect	Clock synchronisation	HML71: Information processing systems, applications, devices, and services are synchronised to an approved time source.	It is important to ensure end point devices are properly synchronised to an approved time source, to ensure accurate logging of incidents, effective operation of SIEM tools, and thorough auditing and review of security incidents. The time source is to be consistent across the organisation's information processing systems. Unsynchronised clocks on the devices across the organisation network are risky and unreliable when log aggregation and SIEM tools are in use to correlate activities for proactive alerting and post incident investigation purposes as the time across systems may not be accurate. So, a standard reference time is to be identified for consideration and use within the organisation, including building management systems, entry and exit systems, and others that can be used to aid investigations. Network time protocol (NTP) and precision time protocol (PTP) are the most commonly used protocols for time synchronisation. A single protocol is recommended for use such that the event logs are accurate during investigations of security incidents or legal and disciplinary cases or medical malpractice to determine clinical sequence of events. While using multiple cloud services, if there is a difference identified in the clock synchronisation, the difference is to be monitored, and the risks which could arise from the variation are to be recorded for consideration.

Appendix A - Glossary

Term	Definition
acceptable use policy	An agreement between two or more parties that outlines the appropriate use of IT assets belonging to an organisation.
asset register	A list of the devices or assets which are used within the organisation and their status of either being in use, in storage or decommissioned.
associated assets	Any asset where information is stored e.g., servers, computers, mobile devices etc.
asymmetric key	A cryptographic system where users have a private key that is kept secret and used to generate a public key (which is freely provided to others). Users can digitally sign data with their private key and the resulting signature can be verified by anyone using the corresponding public key. Also known as a Public-key cryptography.
authentication	Process for establishing an authenticator is genuine or as represented.
authenticator	The means to confirm the identity of a user, process, or device (e.g., user password or token).
authorisation	The rights or permissions granted to a system user to access a system resource.
baseline configuration	A documented set of specifications for an information system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures.
biometrics	Measurable physical characteristics or personal behavioural traits used to identify, or verify the claimed identity of, an individual. Facial images, fingerprints, and handwriting samples are all examples of biometrics.
the Board	Group of people who represent the organisation's and shareholders' interests. They ensure that budgetary responsibilities are met, the workforce is grown, and the infrastructure (both physical and digital assets) are built for the health system.
botnet	A collection of computers linked together to perform a specific task. They can be misused for malicious purposes to control an organisation's computer and use it to carry out attacks on devices outside the network.
break glass account	An account that allows access when other privileged accounts do not authenticate. This account bypasses normal controls and so its credentials are stored offline. Note: break glass does not refer to a medical procedure.

Term	Definition
bring your own device (BYOD)	The practice of allowing employees of an organisation to use their own computers, smartphones, or other devices for work purposes.
business impact analysis	A process and corresponding toolset for identifying those cyber assets that are most critical to the accomplishment of an organisation's mission.
business continuity plan (BCP)	Documented procedures that guide organisations to respond, recover, resume, and restore to a pre-defined level of operation following disruption.
capacity management	Systematic determination of resource requirements for the projected output, over a specific period. These resources are to be monitored and tuned based on the defined requirements such that the required systems or applications or services meet their performance requirements in case of a surge in the number of patients.
certification and accreditation (C&A)	Certification and Accreditation is a fundamental governance and assurance process, designed to provide the Board, Chief Executive and senior executives confidence that information and its associated technology are well-managed, that risks are properly identified and mitigated and that governance responsibilities can demonstrably be met. It is essential for credible and effective information assurance governance. C&A has two important stages where certification is to be completed before accreditation can take place. It is based on an assessment of risk, the application of controls and determination of any residual risk.
certification authority	A trusted entity that issues and revokes public key certificates.
change advisory board (CAB)	A group of personnel who assess, prioritise, authorise and schedule changes. A change manager is usually responsible for organising these meetings (recommended weekly). The CAB is usually made up of representatives from different parts of the organisation, such as IT, security, operations, and business units.
change impact assessment	Is performed by the change owner to predict and anticipate the implications of the proposed changes. These assessments help the decision makers or the CAB to decide on the proposed changes.
change management	Change management is an organised and structured approach with processes or mechanisms that enable organisations to transform workflows seamlessly which evolves along with the sector. Changes are performed when personnel, processes, teams, and tools cannot keep up with the needs and expectations of the organisation’s goals and objectives.

Term	Definition
	This helps to ensure confidentiality, integrity and availability of information.
cloud adoption strategy	Due to the availability of different types of cloud computing deployments, a cloud adoption strategy improves the scalability of Internet-based services while reducing cost and risk. To achieve this, organisations engage in the practice of cloud computing to store, manage and process information via cloud services such as SaaS, PaaS, IaaS. Adoption of a cloud strategy helps organisations to store critical information in the private cloud while leveraging the technological resources from the public cloud to run applications relying on information.
cloud application programming interface (API)	A Cloud API is a software interface that allows developers to link cloud computing services together. APIs allow one computer program to make its data and functionality available for other programs to use. Developers use APIs to connect software components across a network. Cloud APIs are often categorised as being vendor-specific or cross-platform. Vendor-specific cloud APIs are written to support the cloud services of one specific provider, while cross-platform APIs allow developers to connect functionalities from two or more cloud providers.
cloud security risk assessment (CRA)	A tool used by organisations to help them identify and assess the risks arising from the use and handling of PHI and PPII in the cloud. A CRA will also propose ways to mitigate or minimise these risks.
cloud service agreement (CSA)	A cloud services agreement is a legal document between a cloud service provider and a business to use cloud services. This agreement safeguards your organisation by defining what you expect from your cloud service provider (e.g., uptime, security, customer service), and provides terms and conditions for the use of their services.
cloud service provider (CSP)	A cloud service provider is a third-party company offering a cloud-based platform, infrastructure, application, or storage services. Organisations typically have to pay only for the amount of cloud services they use, as healthcare demands require.
code review	Also known as peer reviews, code reviews act as quality assurance of the code base. Code reviews are methodical assessments of code designed to identify bugs, increase code quality, and help developers learn the source code.

Term	Definition
Common Vulnerabilities and Exposure (CVE)	A dictionary of common names for publicly known information system vulnerabilities.
configuration management	A collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initialising, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.
content delivery network (CDN)	This uses a group of servers from different geographic locations to deliver web content online, to ensure that content is available at all times. This makes it hard for an attacker to identify and disrupt the main server.
corrective controls	Include any measures taken to repair damage or restore resources and capabilities to their prior state following an unauthorized or unwanted activity. Examples of technical corrective controls include patching a system, quarantining a virus, terminating a process, or rebooting a system.
cryptography	Art or science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form.
cryptojacking	The act of hijacking a computer to mine cryptocurrencies against the users will, through websites, or while the user is unaware.
cyber security incident	A cyber security event that has been determined to have an impact on the organisation prompting the need for response and recovery.
data loss prevention (DLP)	A systems ability to identify, monitor, and protect data in use, data in motion, and data at rest through deep packet content inspection, contextual security analysis of transaction (attributes of originator, data object, medium, timing, recipient/destination, etc.), within a centralised management framework. Data loss prevention capabilities are designed to detect and prevent the unauthorised use and transmission of sensitive information.
denial-of-service (DOS)	The prevention of authorised access to systems or the delaying of time-critical operations.
detective controls	A detective control is designed to locate problems after they have occurred. Once problems have been detected, management can take steps to mitigate the risk that they will occur again in the future, usually by altering the underlying process. To be truly effective, an organisation needs to follow through on the issues found by its detective controls on an ongoing basis.
deterrent controls	Deterrent controls are administrative mechanisms (such as policies, procedures, standards, guidelines, laws, and regulations) that are used to guide the execution of security within an organisation. Deterrent controls are

Term	Definition
	utilized to promote compliance with external controls, such as regulatory compliance.
development environment	The collection of processes and tools that are used to develop the source code for a program or software product. This involves the entire environment that supports the process end to end, including development, staging and production servers.
differential backup	A data backup that copies all of the files that have changed since the last full backup was performed. This includes any data that has been created, updated or altered in any way and does not copy all of the data every time.
digital certificate	An electronic file that is tied to a cryptographic key pair and authenticates the identity of a website, individual, organization, user, device or server. It is also known as a public key certificate or identity certificate.
discovery scans	A discovery scan identifies the operating systems that are running on a network, maps those systems to IP addresses, and enumerates the open ports and services on those systems.
distributed denial-of-service (DDOS)	A denial-of-service technique that uses numerous hosts to perform the attack to prevent authorised access to systems or the delay of time-critical operations.
domain name server (DNS)	A server that translates requests for human readable names like www.example.com into the numeric IP addresses like 192.0.2.1, controlling which server an end user will reach when they type a domain name into their web browser.
electromagnetic (EM) shielding	The practice of surrounding electronics and cables with conductive or magnetic materials to guard against incoming or outgoing emissions of electromagnetic frequencies (EMF). The most common purpose is to prevent electromagnetic interference (EMI) from affecting sensitive electronics.
encryption	The process of a confidentiality mode that transforms usable data into an unreadable form (ciphertext) using a cryptographic algorithm and key.
encryption key	A key that encrypts other keys for transmission or storage.
endpoint detection and response (EDR)	A solution that continuously monitors end-user devices to detect and respond to cyber threats like ransomware and malware.
environmental security	Examines threats posed by environmental events and trends to organisation personnel.
escrow agreements	An escrow agreement is a legal document outlining terms and conditions between parties as well as the responsibility of each. Agreements usually involve an independent third party called an escrow agent, who holds an asset until the contract's conditions are met.

Term	Definition
ethical hacking	Ethical hackers learn and perform hacking in a professional manner, based on the direction of the client, and later, present a maturity scorecard highlighting their overall risk and vulnerabilities and suggestions to improve.
external libraries	A custom set of functions, objects, and more that were written to eliminate having to write code from scratch. There are hundreds of thousands of external libraries with a vast variety of abilities that they provide. Some of these libraries are part of the standard library.
failback testing	A disaster recovery term which means that a production system is returned to its original state at the new or primary location after a disaster (or scheduled event) is resolved.
failover testing	A disaster recovery term where testing is performed by simulating failure modes or causing failures in a controlled environment. Following a failure, the failover mechanism is tested to ensure that data is not lost or corrupted and that any agreed service levels are maintained (e.g., function availability or response times).
Function as a Service (FaaS)	Also known as serverless computing. In serverless computing, cloud applications are split into smaller components called functions. These functions are run only when required and are billed based on the usage. They are called serverless because, they don't have to run on specific dedicated machines. Serverless functions can scale up easily based on demands.
Government Chief Digital Office (GCDO) 105 questionnaire	A cloud risk assessment tool from the Government Chief Digital Office with 105 questions to be answered. Questions 1 to 27— relate to the information you are looking to use with a public cloud service, find out how important it is to your organisation, the New Zealand government and New Zealanders. Questions 28 to 105 — discover the risks to information security and privacy in a public cloud service and identify the controls to manage them.
information	This includes personal health information (PHI), patient personally identifiable information (PPII), and the implementation of general IT controls within the organisation.
information assets	This includes paper based and digitally stored information, computing devices (e.g., computers, servers, mobile phones), printers, network equipment, specialist medical devices, media storage, that contain information or support the implementation of general IT controls for an organisation.

Term	Definition
high availability	A failover feature to ensure availability during device or component interruptions.
heating, ventilation and air conditioning (HVAC)	The use of technology to treat air by heating, ventilation or cooling.
hybrid cloud	A combination of public and private clouds. Organisations may use a private cloud to store and process their critical information and public cloud for their other services. Some may even use a public cloud as a backup of their private cloud.
incident	A breach of the security rules for a system or service, such as: • attempts to gain unauthorised access to a system and/or data • unauthorised use of systems for the processing or storing of data • changes to a systems firmware, software, or hardware without the system owners' consent • malicious disruption and/or denial of service
incident response plan	The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber-attacks against an organisation's information systems(s).
incremental backup	Successive copies of the data contain only the portion that has changed since the preceding backup copy was made. When a full recovery is needed, the restoration process would need the last full backup plus all the incremental backups until the point of restoration. Incremental backups are often desirable as they reduce storage space usage and are quicker to perform than differential backups.
Infrastructure as a Service (IaaS)	Service that offers on-demand virtualised computing resources such as storage, networking over the internet from a cloud service provider (CSP). The CSP is responsible for maintaining and managing the infrastructure and organisations pay only for the resources which that they consume.
intrusion detection system (IDS)	A monitoring software that looks for suspicious activity and alerts administrators.
intrusion prevention system (IPS)	System which can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its target.
key performance indicators (KPIs)	A quantifiable measure used to evaluate the success of a supplier organisation in meeting objectives for performance in its services delivered to the organisation.
key risk indicators (KRIs)	Defined as measurements, or metrics, used by an organisation to manage current and potential exposure

Term	Definition
	to various operational, financial, reputational, compliance, and strategic risks.
labelled	Information is classified and labelled as internal only, in-confidence, external.
latency	The time it takes for data to pass from one point of the network to another. For example, this could affect how quickly a webpage or application will load for users.
least privilege	The principle that a security architecture is designed so that each entity is granted the minimum system authorisations and resources that the entity needs to perform its function.
legacy systems	Operating systems, applications, internet browsers, computing and network hardware that are out of support by the supplier or manufacturer.
likelihood of occurrence	A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities.
local area network (LAN)	A group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables any device to interact with any other on the network.
log	A record of the events occurring within the organisation's systems and networks.
log analysis	Studying log entries to identify events of interest or suppress log entries for insignificant events.
log retention	Archiving logs on a regular basis as part of standard operational activities.
malicious cyber activity	Activities, other than those authorised by or in accordance with the organisation, that seek to compromise or impair the confidentiality, integrity, or availability of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.
malvertising	A cyber-attack technique that injects malicious code within digital advertisements. Difficult to detect by both internet users and publishers, these infected ads are usually served to consumers through legitimate advertising networks.
malware	Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose.
managed devices	Personal computers, laptops, mobile devices, virtual machines, and infrastructure components require

Term	Definition
	management agents, allowing information technology staff to discover, maintain, and control these devices.
master service agreement (MSA)	Agreement between the organisation and their supplier on the services they will be provided with.
man-in-the-middle (MITM) attack	An attack where the adversary positions himself in between the user and the system so that he can intercept and alter data traveling between them.
media sanitisation	The actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.
message authentication code (MAC)	A string of code that tells you who created or sent a message you received and whether that data has been altered. It does this in a way that validates the sender's identity is legitimate (i.e., a MAC authenticates the sender) over the internet using a shared secret (i.e., a private) key known only by the sender and recipient.
mitigate	A risk management strategy used to minimise the damage or impact of a threat until a problem can be remedied.
mobile device management (MDM)	The administration of mobile devices such as smartphones, tablets, computers, laptops, and desktop computers. MDM is usually implemented through a third-party product that has management features for particular vendors of mobile devices.
multicloud	A kind of deployment where multiple cloud computing services in a single heterogeneous architecture from multiple suppliers are used. It differs from hybrid cloud in that it refers to multiple cloud services, rather than multiple deployment modes (public, private, legacy).
multi-factor authentication (MFA)	Using a combination of multiple authentication factors, such as what you know, what you have and what you are, reduces the possibilities for unauthorised accesses. Multi-factor authentication can be combined with other techniques to require additional factors under specific circumstances, based on predefined rules and patterns, such as access from an unusual location, from an unusual device or at an unusual time.
multi-tenant cloud environment	An organisation that uses the same CSP computing resources between multiple customers. This type of architecture is commonly seen in in many types of public cloud computing including IaaS, PaaS, SaaS, containers and serverless computing.

Term	Definition
need-to-know principle	Decision made by an authorised holder of official information that a prospective recipient requires access to specific official information to carry out official duties.
network access	Access to a system by a user (or a process acting on behalf of a user) communicating through a network, including a local area network, a wide area network, and the Internet.
network access control	A feature provided by some firewalls that allows access based on a user's credentials and the results of health checks performed on the telework client device.
network administrator	A person who manages a network within an organisation. Responsibilities include network security, installing new applications, distributing software upgrades, monitoring daily activity, enforcing licensing agreements, developing a storage management program, and providing for routine backups.
network firewall	Network firewalls are security devices used to stop or mitigate unauthorised access to private networks connected to the Internet, especially intranets. The only traffic allowed on the network is defined via firewall policies — any other traffic attempting to access the network is blocked.
network intrusion detection and prevention systems (NIDS/NIPS)	An intrusion detection and prevention system that monitors network traffic for particular network segments or devices and analyses the network and application protocol activity to identify and stop suspicious activity.
network segmentation	The security of large networks can be managed by dividing them into separate network domains or smaller networks and separating them from the public network (i.e., internet). This helps in limiting the access to only those who need it. The network domains can be separated based on levels of trust, criticality, and sensitivity (e.g., public access domain, desktop domain, server domain, low-risk, and high-risk systems), along with organisational units (e.g., human resources, finance, marketing) or some combination (e.g., server domain connecting to multiple organisational units). The separation can be done using either physically different networks or by using different logical networks.
network sniffing	A passive technique that monitors network communication, decodes protocols, and examines headers and payloads for information of interest. It is both a review technique and a target identification and analysis technique.

Term	Definition
network time protocol (NTP)	An internet protocol used to synchronize with computer clock time sources in a network. The term *NTP* applies to both the protocol and the client-server programs that run on computers.
network virtualisation	Abstracting network resources that were traditionally delivered in hardware to software. Network virtualisation can combine multiple physical networks to one virtual, software-based network, or it can divide one physical network into separate, independent virtual networks.
non-disclosure agreement (NDA)	Delineates specific information, materials, or knowledge that the signatories agree not to release or divulge to any other parties.
non-repudiation	Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.
Open Systems Interconnection (OSI) Model	Seven layers that computer systems use to communicate over a network. It was the first standard model for network communications, adopted by all major computer and telecommunication companies in the early 1980s.
operational controls	The security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems).
open web application security project (OWASP) Top 10	Standard awareness document for developers on web application security issues.
passive scans	A method of vulnerability detection that relies on information gleaned from network data that is captured from a target computer without direct interaction. For an administrator, the main advantage is that it does not risk causing undesired behaviour on the target device, such as freezes. Because of these advantages, passive scanning need not be limited to a narrow time frame to minimize risk or disruption, which means that it is likely to return more information.
password manager	A computer program that allows users to store and manage their passwords for local applications and online services like web applications, online shops or social media.
patch management	The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs.

Term	Definition
patient personally identifiable information (PPII)	Information pertaining to any person which makes it possible to identify such individual. This includes personal characteristics (e.g., height, weight, gender, date of birth, age, ethnicity, place of birth, biometrics information (such as fingerprints, DNA, facial scans) and a unique set of numbers or characters assigned to a specific individual (e.g., name, address, telephone number, NHI number, email address, driver's license number, credit card number and associated PIN number, booking number).
penetration testing	A method of testing where testers target individual binary components or the application as a whole to determine whether intra or intercomponent vulnerabilities can be exploited to compromise the application, its data, or its environment resources.
personal health information (PHI)	Demographic information, medical histories, test and laboratory results, mental health conditions, insurance information and other data that a healthcare professional collects to identify an individual directly or indirectly and determine appropriate care.
personnel	Organisation staff including permanent employees, fixed term employees and temporary roles, contractors, consultants, volunteers, locums, and staff from suppliers who processes or manages information.
personnel security	The discipline of assessing the conduct, integrity, judgment, loyalty, reliability, and stability of individuals for duties and responsibilities requiring trustworthiness.
physical access control system	An electronic system that controls the ability of people or vehicles to enter a protected area by means of authentication and authorisation at access control points.
physical safeguards	Physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorised intrusion.
polymorphic malware	A type of malware that constantly changes its identifiable features in order to evade detection.
privileged account	An information system account with approved authorisations of a privileged user.
Platform as a Service (PaaS)	A cloud computing model where a third-party provider delivers hardware and software tools to users over the internet.
post incident report (PIR)	Provides a summary of an incident along with the lessons learnt.

Term	Definition
preventive controls	A control that is put into place and intended to avoid an incident from occurring. The point of preventive control is to stop any trouble before it starts.
Private cloud	The cloud infrastructure is provisioned for exclusive use by a single organisation comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organisation, a third party, or some combination of them, and it may exist on or off premises.
privileged access	Permissions that enable one or more of: • the ability to change key system configurations • the ability to change control parameters • access to audit and security monitoring information • the ability to circumvent security measures • access to all data, files and accounts used by other system users, including backups and media or • special access for troubleshooting the system.
privileged account	An account that is used almost exclusively to perform actions based on privileged access. In almost all cases a privileged user account will be issued to individuals with a standard user account (which is used for day-to-day) purposes.
production environment	Environment where there is where there is latest versions of software, products, or updates are pushed live to the intended users
public cloud	The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organisation, or some combination of them. It exists on the premises of the cloud provider.
public key and private key	Public and private keys are two very large numbers that (through advanced mathematics) have a unique relationship, whereby information encrypted with one number (key) can only be decrypted with the other number (key) and vice versa. In order to leverage this characteristic for security operations, once two numbers are mathematically selected (generated), one is kept secret (private key) and the other is shared (public key). The holder of the private key can then authenticate themselves to another party who has the public key. Alternatively, a public key may be used by one party to send a confidential message to the holder of the

Term	Definition
	corresponding private key. With SSH, the identity key is a private key and authorised keys are public keys.
public key certificate	A digital representation of information which at least • identifies the certification authority (CA) issuing it, • names or identifies its subscriber, • contains the subscriber's public key, • identifies its operational period, and • is digitally signed by the certification authority issuing it.
ransomware attack	A type of malware that prevents you from accessing your computer (or the data that is stored on it). The computer itself may become locked, or the data on it might be stolen, deleted or encrypted.
RASCI matrix	A Responsible, Accountable, Supporting, Consulted, Informed (RACI) matrix is a tool that can support clarity on job roles and responsibilities. It is used to map out and document the key activities and deliverables for a function and the individuals or groups that have responsibility for their completion, signoff, and awareness.
recovery point objective (RPO)	Maximum amount of data the organisation can tolerate losing.
recovery time objective (RTO)	The maximum length of time it is to take to restore normal operations following an outage or data loss.
remediation	Implementing corrective action to eliminate a risk.
remote access	Access to an organisation's information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet).
remote desktop protocol (RDP)	A proprietary protocol by Microsoft which helps personnel to connect to their or a specific work device when they work remotely.
remote working	Remote working is one type of flexible working. It is the practice of employees doing their jobs from a location other than a central office operated by the employer.
removable storage media	A system component that can communicate with and be added to or removed from a system or network and that is limited to data storage—including text, video, audio or image data—as its primary function (e.g., optical discs, external or removable hard drives, external or removable solid-state disk drives, magnetic or optical tapes, flash memory devices, flash memory cards, and other external or removable disks).

Term	Definition
residual risk rating	The measurement of risk (impact x likelihood) with suitable controls in place.
risk	Security problems that an organisation could potentially face.
risk analysis	The process of identifying risks to an organisation's operations (including mission, functions, image, reputation), organisational assets, individuals, other organisations, resulting from the operation of a system.
risk assessment matrix	A tool used during the risk assessment stage of project planning. This tool simplifies the information from the risk assessment form, making it easier to pinpoint major threats in a single glance. This convenience makes it a key tool in the risk management process, as it helps organisations make decisions faster and more easily.
risk assessment methodology	A risk assessment process, together with a risk model, assessment approach, and analysis approach.
risk evaluation	Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is/are acceptable or tolerable.
risk identification	Process of finding, recognizing, and describing risks.
risk management plan	Document that a project manager prepares to foresee risks, estimate impacts, and define responses to risks. It also contains a risk assessment matrix.
risk register	A central record of current risks and related information for a health provider organisation. Current risks comprise of both accepted risks and risks that have planned mitigation activities in place.
risk treatment	Process to modify risk.
role-based access control (RBAC)	Access control based on user roles (i.e., a collection of access authorisations that a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within the organisation. A given role may apply to a single individual or to several individuals.
rootkits	Software(s) used by cybercriminals to gain control over a target computer or network.
root cause analysis	A principle-based, systems approach for the identification of underlying causes associated with a particular set of risks.
safeguards	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management

Term	Definition
	constraints, personnel security, and security of physical structures, areas, and devices.
sandbox environment	A restricted, controlled execution environment that prevents potentially malicious software, from accessing any system resources except those for which the software is authorised.
sanitisation	Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.
secure coding	Writing code in a high-level language that follows strict principles, with the goal of preventing potential vulnerabilities.
security architecture	A set of physical and logical security-relevant representations (i.e., views) of system architecture that conveys information about how the system is partitioned into security domains and makes use of security-relevant elements to enforce security policies within and between security domains based on how data and information is to be protected. The security architecture reflects security domains, the placement of security-relevant elements within the security domains, the interconnections and trust relationships between the security-relevant elements, and the behaviour and interaction between the security-relevant elements. The security architecture, similar to the system architecture, may be expressed at different levels of abstraction and with different scopes.
security audit	Independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures.
security awareness training	Programs designed to help users and employees understand the role they play in helping to combat information security breaches.
security control	A safeguard or countermeasure to avoid, detect, counteract, or minimise security risks to physical property, information, computer devices, or other assets. Such controls protect the confidentiality, integrity, and availability of information.
security engineering	An interdisciplinary approach and means to enable the realisation of secure systems. It focuses on defining customer needs, security protection requirements, and required functionality early in the systems development lifecycle, documenting requirements, and then proceeding with design, synthesis, and system validation while considering the complete problem.

Term	Definition
security incident	An occurrence that actually or potentially jeopardises • the confidentiality, integrity, or availability of an information system or • the information the system processes, stores, or transmits or • that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
security information and event management (SIEM)	A solution that helps organisations detect, analyse, and respond to security threats before they harm business operations. SIEM combines both security information management (SIM) and security event management (SEM) into one security management system. SIEM technology collects event log data from a range of sources, identifies activity that deviates from the norm with real-time analysis, and takes appropriate action. In short, SIEM gives organisations visibility into activity within their network so they can respond swiftly to potential cyberattacks and meet compliance requirements. In the past decade, SIEM technology has evolved to make threat detection and incident response smarter and faster with artificial intelligence. SIEM Tool: Application that provides the ability to gather security data from information system components and present that data as actionable information via a single interface.
security policy	A set of rules that governs all aspects of security-relevant system and system component behaviour.
security review	A collaborative process used to identify security-related issues, determine the level of risk associated with those issues, and make informed decisions about risk mitigation or acceptance.
security risk assessment (SRA)	The process of identifying risks to a health provider organisation's operations, assets, or individuals by determining the probability of occurrence, the resulting impact and additional security controls that would mitigate
security risk management plan (SRMP)	A foundation document which communicates the issues that are important to an organisation from a security risk management perspective and to address the issues.
serverless computing	A method of providing backend services on an as-used basis. Servers are still used, but a company that gets backend services from a serverless vendor is charged

Term	Definition
	based on usage, not a fixed amount of bandwidth or number of servers.
service account	Digital identity used by an application software or service to interact with other applications or the operating system.
service level agreement (SLA)	Represents a commitment between a service provider and one or more customers and addresses specific aspects of the service, such as responsibilities, details on the type of service, expected performance level (e.g., reliability, acceptable quality, and response times), and requirements for reporting, resolution, and termination.
service organisation controls (SOC) report	A way to verify that an organisation is following some specific best practices before you outsource a business function to that organisation.
service provider	A provider of basic services or value-added services for operation of a network, generally refers to public carriers and other commercial enterprises.
shared responsibility model	A security and compliance framework that outlines the responsibilities of cloud service providers (CSPs) and customers for securing every aspect of the cloud environment, including hardware, infrastructure, endpoints, data, configurations, settings, operating system (OS), network controls and access rights.
side-channel attack	An attack enabled by leakage of information from a physical cryptosystem. Characteristics that could be exploited in a side-channel attack include timing, power consumption, and electromagnetic and acoustic emissions.
single sign-on (SSO)	An authentication method that enables users to securely authenticate with multiple applications and websites by using just one set of credentials.
site plan	The physical security equivalent of the SSP and SOPs for systems, are used to document all aspects of physical security for systems. Formally documenting this information ensures that standards, controls and procedures can easily be reviewed by security personnel.
stakeholders	Includes internal staff, suppliers, patients, the Board, Te Whatu Ora.
standard user account	A day-to-day account used by: • employees • contractors • suppliers • business / technical consultants These accounts are provided to the individual users in order for them to access information on the organisation's network. Standard user accounts are linked to a single person.

Term	Definition
social engineering	The act of deceiving an individual into revealing sensitive information, obtaining unauthorised access, or committing fraud by associating with the individual to gain confidence and trust.
Software as a Service (SaaS)	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
software asset management	A capability that identifies unauthorised software on devices that is likely to be used by attackers as a platform from which to extend compromise of the network to be mitigated.
software bill of materials (SBOM)	The inventory of components used to build a software artefact such as a software application.
software defined network (SDN)	An approach to network management that enables dynamic, programmatically efficient network configuration in order to improve network performance and monitoring, making it more like cloud computing than traditional network management.
software development lifecycle (SDLC)	A formal or informal methodology for designing, creating, and maintaining software (including code built into hardware).
software firewall	A software-based firewall installed on a desktop or laptop computer to provide protection against external cyber attackers by shielding the computer from malicious or unnecessary network traffic. A software firewall can also prevent malicious software from accessing a computer via the internet.
spyware	Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organisations without their knowledge; a type of malicious code.
SQL injection	Attacks that look for web sites that pass insufficiently processed user input to database back-ends.
strong authentication	A method used to secure computer systems and/or networks by verifying a user's identity by requiring two-factors in order to authenticate (something you know, something you are, or something you have).
supplier account	An account used by a supplier to access the systems and devices on their customer's network.

Term	Definition
supply chain	Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer.
supply chain assurance	Confidence that the supply chain will produce and deliver elements, processes, and information that function as expected.
supply chain risk	The potential for harm or compromise that arises as a result of security risks from suppliers, their supply chains, and their products or services. Supply chain risks include exposures, threats, and vulnerabilities associated with the products and services traversing the supply chain as well as the exposures, threats, and vulnerabilities to the supply chain.
supply chain risk assessment	A systematic process for managing cyber supply chain risk exposures, threats, and vulnerabilities throughout the supply chain and developing risk response strategies to the risks presented by the supplier, the supplied products and services, or the supply chain.
supply chain risk management (SCRM)	The process of identifying, assessing, and mitigating the risks of organisations provider's supply chain.
system assurance	The justified confidence that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during the life cycle.
system hardening	Collection of tools, techniques, and best practices to reduce vulnerability in technology applications, systems, infrastructure, firmware, and other areas.
system security plan (SSP)	Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.
supplier	Service provider of on-premises or cloud services. e.g., Internet Service Provider, Outsourced Service Provider, Software as a Service (SaaS) provider.
symmetric key	One key that is used to encrypt and decrypt the information.
tabletop exercise	A discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular

Term	Definition
	emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario.
tampering	An intentional but unauthorised act resulting in the modification of a system, components of systems, its intended behaviour, or data.
target residual risk	The amount of risk that an entity prefers to assume in the pursuit of its strategy and business objectives, knowing that management will implement, or has implemented, direct or focused actions to alter the severity of the risk.
technical security controls	Security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.
test environment	Environment where testing teams analyse the quality of the application/program.
threat	Any event with the potential to adversely impact organisational operations, organisational assets, individuals, other organisations, through an information system via unauthorised access, destruction, disclosure, modification of information, and/or denial of service.
threat and vulnerability assessment (TVA)	Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.
threat intelligence	Threat information that has been aggregated, transformed, analysed, interpreted, or enriched to provide the necessary context for decision-making processes.
threat modelling	A form of risk assessment that models aspects of the attack and defence sides of a logical entity, such as a piece of information, an application, a host, a system, or an environment.
transport layer security (TLS)	A security protocol providing privacy and data integrity between two communicating applications. The protocol is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol.
trojans	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorisations of a system entity that invokes the program.

Term	Definition
tunnelling	Technology enabling one network to send its data via another network's connections. Tunnelling works by encapsulating a network protocol within packets carried by the second network.
two-factor authentication (2FA)	Authentication using two or more factors to achieve authentication. Factors include: • something you know (e.g., password/personal identification number [PIN]) • something you have (e.g., cryptographic identification device, token) or • something you are (e.g., biometric).
user and entity behaviour analytics (UEBA)	A type of cyber security process that takes note of the normal user behaviour. In turn, they detect any anomalous behaviour or instances when there are deviations from these "normal" patterns. For example, if a particular user regularly downloads 10MB of files every day but suddenly downloads gigabytes of files, the system would be able to detect this anomaly and alert the administrator or manager immediately.
unauthorised access	A person gains logical or physical access without permission to a network, system, application, data, or other resource.
uninterruptible power supply (UPS)	A device with an internal battery that allows connected devices to run for at least a short time when the primary power source is lost.
virtual local area network (VLAN)	A broadcast domain that is partitioned and isolated within a network at the data link layer. A single physical local area network (LAN) can be logically partitioned into multiple, independent VLANs; a group of devices on one or more physical LANs can be configured to communicate within the same VLAN, as if they were attached to the same physical LAN.
virtual machine (VM)	A virtual data processing system that appears to be at the disposal of a particular user but whose functions are accomplished by sharing the resources of a real data processing system.
virtual private network (VPN)	A virtual network built on top of existing physical networks that can provide a secure communications mechanism for data and IP information transmitted between networks or between different nodes on the same network.
visitor management system	Process of tracking everyone who enters your building or your office.

Term	Definition
vulnerability	A weakness, or flaw, in software, a system or process. An attacker may seek to exploit a vulnerability to gain unauthorised access to a system.
vulnerability assessment/scan	A systematic review of security weaknesses in an information system. It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities and recommends remediation or mitigation, if and whenever needed.
vulnerability management	The ongoing, regular process of identifying, assessing, reporting on, managing and remediating cyber vulnerabilities across endpoints, workloads, and systems. Typically, a security specialist would leverage a vulnerability management tool to detect vulnerabilities and utilise different processes to patch or remediate them.
web application firewall (WAF)	A layer 7 firewall that protects web applications against common web exploits, cyber-attacks, and bots that can compromise the security and affect the availability of information and associated services.
whitelist	A list of discrete entities, such as hosts, email addresses, network port numbers, runtime processes, or applications that are authorised to be present or active on a system according to a well-defined baseline.
Wi-Fi network	A generic term that refers to a wireless local area network.
worm	Subset of the trojan horse malware that can propagate or self-replicate from one computer to another without human activation after breaching a system.
zero trust	A collection of concepts and ideas designed to minimise uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.