Te Whatu Ora
Health New Zealand

hiso
Health Information Standards Organisation
PAEREWA PĀRONGO HAUORA

Health Information Security Framework Guidance for Suppliers

HISO 10029.4:2023

Released August 2023

Te Kāwanatanga o Aotearoa
New Zealand Government

Citation: Te Whatu Ora – Health New Zealand. 2022. *HISO 10029.4:2023 Health Information Security Framework for Suppliers*. Wellington: Te Whatu Ora – Health New Zealand.

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

ISBN 978-1-99-106746-3 (online)

Health Information Standards Organisation (HISO) standards are published by the Ministry of Health for the New Zealand health and disability system.

Te Whatu Ora
Health New Zealand

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

Contents

Purpose

This document is published as part of the Health Information Security Framework (HISF) to provide cyber security guidance for suppliers, who are defined as a service provider of on-premises or cloud services. e.g., internet service provider, outsourced service provider, software as a service (SaaS) provider to the health sector.

Implementation of the Health Information Security Framework within the supplier 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 the suppliers,
- using HISF tools, templates and other approved materials to meet the requirements outlined in 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 the supplier segment 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 implementing controls 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 suppliers

The list below contains cyber security requirements for suppliers abbreviated as HSUP (HISF Suppliers). The requirements are grouped according to the five HISF functional processes as defined in section **5 HISF Framework** from the **core framework document**.

	PLAN
HSUP01	The organisation has a clear information security policy, acceptable use policy, topic-specific policies and procedures to maintain information security.
HSUP02	Security roles and responsibilities of personnel are included within job descriptions.
HSUP03	A breach of information by personnel is considered a security policy violation. Consequences of a security policy violation leads to a disciplinary process.
HSUP04	There are documented procedures for providing and revoking logical, and physical access when personnel join, have a role change or leave the organisation.
HSUP05	Asset management process(es) are in place.
HSUP06	Processes are in place for media equipment management, decommissioning and secure disposal.
HSUP07	An information security incident management process is in place.
HSUP08	Organisations have a documented, approved, business continuity and disaster recovery management, operational resilience policies and procedures in place.
HSUP09	Establish, document, approve, and implement rules to control physical and logical access to information and its assets.
HSUP10	The organisation's Board or information security steering committee is accountable for information security governance.
HSUP11	A documented policy and supporting procedures for maintaining physical security within the organisation is in place.
HSUP12	A documented and approved procedure to remove papers and removable storage from easily accessible areas is to be implemented.
HSUP13	Organisations have planned maintenance of information and services that are being provided to their customers via cloud services as per documented policies and agreements.

HSUP14	Information systems are securely designed, and appropriate controls are implemented.
HSUP15	A backup and recovery procedure is in place.
HSUP16	A documented process is in place for performing changes to new and existing systems or services.
HSUP17	There is a documented and approved process for identifying vulnerabilities and updating patches on the organisation's systems, applications, tools, services etc.
	IDENTIFY
HSUP18	Organisations, at a minimum, screen all personnel by verifying their identity, previous employment, applicable professional qualifications and criminal backgrounds before confirmation of employment.
HSUP19	Organisations are to ensure: • information security responsibilities are clearly defined and assigned • a governance body or steering committee overseeing information security activities is in place • there is at least one individual responsible for maintaining information security within the organisation.
HSUP20	There has been an assessment of information security training needs and a training plan is put in place.
HSUP21	Organisations are to have roles and responsibilities determined to carry out the incident management process.
HSUP22	Establish criteria for developing business continuity, disaster recovery, operational resilience strategies, and capabilities based on disruption and impact to the organisation.
HSUP23	Roles and responsibilities are defined and documented for planning, implementing, operating, assessing, and reporting on the organisation's information security requirements.
HSUP24	Organisations are to integrate information security into project management.
HSUP25	Relevant legal, regulatory, and contractual requirements are identified and implemented.
HSUP26	A risk assessment methodology and cloud assurance activities that support the use of cloud technologies are in place.
HSUP27	Business, customer, and security requirements are identified, documented, and approved when developing or acquiring applications.
HSUP28	Risk assessments are performed on new, existing systems, and applications to understand the risks posed to the organisation while using them.
HSUP29	The proposed changes are to be analysed for potential security threats and their impact on the organisation and their customers.

PROTECT	
HSUP30	The organisation’s information and associated assets are appropriately protected, used, and handled based on their importance.
HSUP31	In the event of a disruption or failure, critical information or services are identified, and measures are taken for the continuity of services.
HSUP32	Rules for effective use of cryptography, including encryption, and key management are defined and implemented.
HSUP33	The complete lifecycle of the account(s) being used to access, process, or manage information and services is managed.
HSUP34	User accounts are authenticated and circumventing the authentication process is prevented.
HSUP35	Access to information and its associated assets is defined and authorised according to the business, customer and security requirements by adhering to the organisation’s identity and access management policy or procedures.
HSUP36	Organisations are to ensure that only authorised users, software components and services are provided with privileged access rights.
HSUP37	Access to source code, development tools, and software libraries are restricted, appropriately managed, and maintained.
HSUP38	Metrics affecting the organisation’s cyber security posture are regularly reported to the Board, and any decisions made are clearly documented.
HSUP39	Update, protect and maintain the devices installed as physical security safeguards including the utilities.
HSUP40	Secure areas of the organisation are protected from unauthorised personnel.
HSUP41	Secure mechanisms are available and supported by a documented policy or guidelines to connect to the organisation’s or customer’s network.
HSUP42	Security controls are implemented if the organisation is developing the web applications to protect them and their customers from potential cyber-attacks.
HSUP43	The organisation's architectural strategy supports the adoption of cloud technologies.
HSUP44	Organisations are to make use of developed and configured APIs for secure transfer of information between different cloud components.
HSUP45	Organisations are to ensure that appropriate controls are implemented to protect information in a multi-tenant cloud environment.
HSUP46	Networks and network devices that are used within the organisation are to be securely managed.

HSUP47	The systems and applications that are used to process, store, or transmit information are connected to a separate, dedicated network.
HSUP48	Backup copies of information, software, services provided, and relevant systems are protected and maintained in accordance with the backup and recovery procedures.
HSUP49	Backups are tested for their restoration in accordance with the documented backup and recovery procedures. Organisations are able to access restored backups as well.
HSUP50	Organisations developing inhouse systems, applications, or services are to maintain separate production and non-production environments.
HSUP51	Identified vulnerabilities or unpatched systems, services or applications are properly identified, tracked, and remediated.
HSUP52	Organisations have a standardised baseline configuration in place for new and existing systems, services, and applications.
HSUP53	The capacity requirements for maintenance of information processing facilities, communication, and environmental support during contingency operations are met.
HSUP54	Information, services, and applications on organisation systems and associated assets are protected against malware.
HSUP55	Organisations are to detect and prevent data leakage through the unauthorised disclosure and siphoning of information by individuals, systems, or services.
DETECT	
HSUP56	The lessons learned from business continuity and disaster recovery testing are reflected in the established and implemented information security controls.
HSUP57	Installed physical and environmental security mechanisms are monitored for potential security incidents.
HSUP58	Regular reviews are performed to confirm that the legal, regulatory, statutory, and contractual requirements are met.
HSUP59	Independent security reviews are defined and implemented before any new or major upgrades on systems are moved to the production environment.
HSUP60	Authorised personnel or teams are alerted upon unsuccessful backups.
HSUP61	The activities performed on the information processing systems, services, and applications are logged and stored as per the organisation’s (and the customer’s) logging and auditing requirements.

HSUP62	The information processing systems, applications, devices, and services are synchronised to an approved time source.
RESPOND	
HSUP63	Breach of employment and supplier agreements are enforced.
HSUP64	Misuse of the organisation’s assets is investigated, and documented procedures are followed as stated in the acceptable use policy, contractor agreements, or service agreements.
HSUP65	Organisations report all security incidents and near misses to their senior management or to the Board by a nominated Information Security Officer. All customer-related incidents are to be notified to the customer as per agreed timelines.
HSUP66	Evidence gathered as part of the incident management process is appropriately protected.

Requirements and guidance for suppliers

Functional Process	Control Area	Requirement	Guidance
Information security policy Implementation of controls in this section ensures that there is a continuous effective management direction and support for security of information in accordance with their business, legal, regulatory, and contractual requirements.			
Plan	Policies for information security	HSUP01: The organisation has a clear information security policy, acceptable use policy, topic-specific policies and procedures to maintain information security.	**Organisation's policies** An "information security policy" sets out the supplier's approach in managing their information security, while an "acceptable use policy" communicates the acceptable use of organisational, customer information and its associated assets. These policies are to be defined, approved by senior management, communicated to all relevant personnel and reviewed periodically. **Information security policy** While documenting an information security policy to manage organisational and customer 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 • 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 stakeholders (i.e., customers in health sector, etc.) • processes and procedures for notification of potential and actual information security incidents, including but not limited to a channel for raising concerns regarding confidentiality, integrity, or availability, without fear of blame or accusation • the identification of processes and systems that are vital in organisational services supporting its customers within the health sector (i.e., failure may lead to adverse patient effects). **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 other associated assets • monitoring activities being performed by the organisation.

Functional Process	Control Area	Requirement	Guidance
			Acceptable use procedures are to be drawn up for the full life cycle of information in accordance with the classification and risks determined. While documenting, consider: • definition of the information to be protected and what constitutes its acceptable use • required access restrictions that support the protection of information based on its classification • maintenance of a record of the authorised users • protection of temporary or permanent copies (e.g., printouts, USBs, local copies on laptops or desktops) of information to a level consistent with the protection of the original • storage of information assets associated with services that are being provided to customers in accordance with the agreed terms and conditions or as per documented agreements • 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 • the permitted use of information and usage rights of the signatory • the right to audit and monitor activities on organisational devices • 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 with the agreement. The policy documents are to be made available to personnel electronically via a secure area on the organisation's intranet for reference purposes. **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 security groups, stakeholders within and outside the organisation. Topic-specific policies are to be aligned with, and complementary to the information security policy of the supplier. 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 these policies are to be allocated to relevant authorised personnel based on their appropriate level of authority and technical competency (i.e.,

Functional Process	Control Area	Requirement	Guidance
			business/risk owner). The review cycle is to include assessing opportunities for improvement of these policies when there are changes in: • the supplier's business and security strategy • the supplier'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 all the developed policies and procedures is to follow a set schedule or be driven by the results of the risk assessments, or 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 policies, consider: • the changing nature of the organisation's operations and the associated changes to risk profile and risk management needs • the changes made to the IT, security and business architecture 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 professional associations, such as the NZ privacy commissioner regarding the protection of organisational information and organisations, Emergency Care Research Institute (ECRI) on 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 • any challenges and issues regarding implementing the policy, as expressed by the organisation personnel, their customers (i.e., customers within the health sector), researchers and government bodies (e.g., the NZ privacy commissioner) • patient safety for the customers within the health sector, technology, processes, health information/records security and respective mitigation strategies to protect against the failure of information security measures. Any changes made to these documents are to be approved by senior management.

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 and • protect the organisation's interests when there is a change of role.			
Plan	Terms and conditions of employment	HSUP02: 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 topic-specific policies. In addition, the agreements are to cover: • confidentiality or non-disclosure agreements are 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 managing and handling information, its associated assets, information processing facilities and services handled by the personnel • responsibilities to report breaches of information security or customer information or to the incident management team within a specific timeframe • actions to be taken if personnel breach the organisation's security requirements. **Roles and responsibilities** Information security roles and responsibilities are communicated to candidates during pre-employment or as part of the onboarding process. The organisation ensures that personnel agree to terms and conditions concerning information security which are appropriate to the nature and extent of access they will have. The terms and conditions concerning information security are reviewed when laws, regulations, the information security policy, or topic-specific policies changes. Security responsibilities are also included in the job descriptions of all personnel as it is everyone's responsibility.
Plan	Terms and conditions of employment	HSUP03: A breach of 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 incident was intentional (malicious) or unintentional (accidental) • whether or not this is a first or repeated incident • whether or not the employee 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

Functional Process	Control Area	Requirement	Guidance
			deterrent to prevent personnel and other relevant parties from violating the information security policy, topic-specific policies, and procedures for information security. Deliberate information security policy violations may require immediate action. Where possible, the identity of individuals subject to disciplinary action is to be protected.
Plan	Onboarding, offboarding and role change	HSUP04: There are documented procedures for providing and revoking logical, and physical access when personnel join, have a role change or leave the organisation.	**Documented procedures** Documented user access creation, modification and deletion procedures clearly identify whether personnel: • have access to 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, long leave) • have access to the premise (including devices, applications, tools) 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 is 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 the information and its associated assets (in particular ensuring access rights of users who have left the organisation are removed) • 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)

Functional Process	Control Area	Requirement	Guidance
			• 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 support during incidents, as they may need access to information in emergency situations. 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 and to be actioned in a timely manner. **Access reviews** Regular reviews of physical and logical access rights are to consider: • users' access rights after any change within the same organisation (e.g., job 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 the supply of a resignation notice, notice of dismissal, etc.
Identify	Terms and conditions of employment	HSUP18: Organisations, at a minimum, screen all personnel by verifying their identity, previous employment, applicable professional qualifications and criminal backgrounds before confirmation of employment.	**Hiring process** Where personnel are directly hired by the organisation (or contracted through other suppliers or recruitment agencies), a documented and approved screening process is to be followed before providing access to the organisation's information and infrastructure. For individuals contracted through other suppliers, screening requirements are included in the contractual agreements between the organisation and other 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, includes: • 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 • Police checks

Functional Process	Control Area	Requirement	Guidance
			• Credit checks for applicable roles • independent identity verification (e.g., passport or other acceptable document issued by appropriate authorities) 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 to the organisation • clearly understands the security expectations of the role and their obligations towards their organisation and its customers. Where a role, either through appointment or subsequent promotion, involves the person having a change of access to information, the organisation is to consider more detailed verifications based on the new roles and responsibilities. Procedures are to define criteria and 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 in every 3 years and annually for privileged users (i.e., system administrators, etc) to confirm ongoing suitability of access. **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 reputable 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 code of conduct and the organisation's Acceptable Use Policy as part of the 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 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 the suppliers 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	HSUP19: Organisations are to ensure: • information security responsibilities are clearly defined and assigned • a governance body or steering committee overseeing information security activities is in place • there is at least one individual responsible for maintaining information security within the organisation.	**Roles and responsibilities** Organisations are to have 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 the organisation adopts, it is critical that it's designed and structured to facilitate appropriate access to information, reporting within the organisational structure and to ensure timely delivery of information and applicable services to its customers. 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 accountable and are to ensure that the delegated tasks have been correctly performed. Each security (information, personal, physical) area for which personnel are responsible and authorisation levels are to be defined, documented, communicated and reviewed periodically. Personnel who take on a specific security role are to be competent in the knowledge and skills required by the role and is to be supported to keep up to date with developments related 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 types of services that are being provided. 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, neither is the creation of the group be taken as a mandate to create "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 the services which are being provided to the customers, 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

Functional Process	Control Area	Requirement	Guidance
			nature of information security within information governance makes the positioning of the group within the information governance structure a sensible arrangement. Taking an information governance approach underscores the critical nature of information security and allows an integrated process, with risk analysis input, that directly feeds into overall 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 appointed CISO is to ensure that the information security governance 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 all personnel and the corporate governance body • 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 recommendation 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 supplier 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 • helps the organisation comply with their security policies, external regulatory and legal requirements • determines if and how security is adequate

Functional Process	Control Area	Requirement	Guidance
			• conducts regular audits to help the organisation meet their security and business objectives (recommended every quarter).
Identify	Training Requirements	HSUP20: 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 on information security. 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 and its associated assets • 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 and multi-factor authentication) • contact points and resources for additional information and advice on information security matters, including further awareness materials. • individuals having at least adequate knowledge of the various management, operational, and technical controls required and available to protect the IT resources for which they are responsible. 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, for example 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 skill sets and expertise (e.g., biomedical teams for the clients within the health sector and technical teams need the skills for configuring and maintaining the required security level

Functional Process	Control Area	Requirement	Guidance
			for biomedical devices, corporate devices, systems, applications, and services). 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 information over, insecure networks. **Leadership roles** The organisation's risk profile and threat landscape (identified as part of 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	HSUP63: 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. 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 organisations and customers (if applicable) 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 for the

Functional Process	Control Area	Requirement	Guidance
			communication of the changes and of operating procedures to relevant personnel, and relevant contact persons (e.g., to customers and suppliers). The process for the termination or change of employment is to also be applied to suppliers when a termination occurs of their personnel, their contract, or the job with their organisation, or when there is a change of the job or role within their 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 relevant procedures. 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 contract between the supplier 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 customer 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	HSUP05: Asset management process(es) are in place.	**Asset management process** Organisations are to manage a documented and approved process to procure, maintain and dispose 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 the 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. Devices that record or report data (e.g., medical devices) may require special security considerations in relation to the environment in which they operate and are 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 the identified information and its associated assets, 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 when assets are transferred to the organisation. Asset ownership is to be reassigned as necessary when current asset owner leaves or change job roles. **Ownership of assets** The organisation is to identify its information assets, associated infrastructure and determine their importance based on the level of information security and its owner. Documentation is to be maintained for dedicated or existing inventories. 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 capture, processing, transfer, storage or recall of information. This includes all on and off premise devices or as a service platform 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

Functional Process	Control Area	Requirement	Guidance
			• include rules for maintaining the currency of assets and their integrity (e.g., the functional integrity of devices that record or report information and the services that are being provided to their customers). The asset owner is to be 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 of managing information within the asset(s). **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 is to be in conjunction with the organisation or customer's assets (e.g., through agreements with cloud service providers or mobile device management). Care is to be taken when a collaborative working environment is used.
Plan	Media Equipment Management, Decommissioning and Disposal	HSUP06: 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., as per contractual agreements with customers) from the premise. An approval process is in place to take these assets out of the organisation for repairs or disposal activities. An overarching approval for specific roles within the organisation could be provided for the movement of assets. 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. **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. **Removable storage media** Organisations processing, managing or storing information on removable storage media are to consider:

Functional Process	Control Area	Requirement	Guidance
			• establishing a topic-specific policy or procedure and communicating it 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 protecting them 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 devices, unless there is a documented 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 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 personal 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 needs 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 containing securely when not needed anymore (e.g., by destroying, shredding, or securely deleting the content) • having procedures in place that require secure disposal • many organisations offer collection and disposal services for storage media. Care is to be taken in selecting a suitable external party supplier with adequate controls and experience • logging the disposal of devices on which information is stored to maintain an audit trail • a secure disposal certificate stating that the agreed procedures were followed is stored and maintained for reference purposes • 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 to be performed on damaged devices containing information to determine whether the items are to be physically destroyed rather than sent for repair or discarded.

Functional Process	Control Area	Requirement	Guidance
			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	HSUP30: The organisation's 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 is to be performed to identify, reduce the risks from physical and environmental threats and from unauthorised access and damage which may be caused while protecting these assets. A minimum of the following guidelines is to be considered to protect assets: • siting equipment and information processing facilities to minimise unnecessary access into work areas and to avoid unauthorised access (e.g., CCTV surveillance, server rooms, etc) • 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, and vandalism) • establishing guidelines for eating, drinking, and smoking in proximity to information processing facilities • monitoring environmental conditions (such as 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 (such as keyboard membranes), for equipment in industrial 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 • risk assessments performed are to also address the potential impacts to the customer information and the services that are being provided • 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 allowing access to information in a way that prevents unintended viewing or access by unauthorised parties. Organisations are to ensure 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 • 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 which are used to store, process, or transmit information from actions or events that can cause damage to

Functional Process	Control Area	Requirement	Guidance
			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 either encrypted, changed, or completely disabled so that usernames and passwords are not easily guessed by hackers.
Respond	Information and associated assets	HSUP64: Misuse of the organisation's assets is investigated, and documented procedures are followed as stated in the acceptable use policy, contractor agreements, or service agreements.	**Information security requirements** Apart from the existing requirements within the organisation, additional information security requirements that are being provided or requested by the customer are to be identified and implemented. Personnel accessing customer information and its associated assets are to be made aware of specific information security requirements, if any. 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 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 for the full information life cycle (in accordance with its protection requirements, including potential risks) while considering: • access restrictions supporting the protection requirements for information • maintenance of a record of the authorised users of information and its associated assets • protection of temporary or permanent copies of information (to a level consistent with the protection requirement 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 and supported deletion method(s).

Functional Process	Control Area	Requirement	Guidance
Information security incident management Implementation of controls in this section ensures that there is: • an effective and efficient response to the customer's information security incidents to reduce likelihood or consequences of future incidents • consistent and effective management of evidence related to the incidents for the purposes of disciplinary and legal actions.			
Plan	Planning and preparation	HSUP07: 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, customers and is to be ensured that those responsible for information security incident management understand the priorities for handling incidents (including resolution time frame based on potential consequences and severity). Incident management procedures are to be implemented to meet these objectives and priorities. 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 could 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. **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 information breaches, and vulnerabilities) and the point of contact for reporting these. If there are events identified at the customer end, a channel is to be established to report those incidents. 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 • 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 which is being provided to their customers (and it can corrupt or obscure digital evidence). Ultimately, this can result in legal liability for the individual performing the testing.

Functional Process	Control Area	Requirement	Guidance
			Testing of information security incident management process Regular tabletop 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 to carry out the incident management procedures between internal teams and customers. These are to be effectively communicated to the relevant internal and external stakeholders • 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, and 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 reviews, and external reporting obligations (specifically 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 after an incident review). **Information security incident management plan** Organisation's management are to ensure that an information security incident management plan is created considering different scenarios (including customer information) and procedures are developed and implemented for the following activities: • regular tabletop 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

Functional Process	Control Area	Requirement	Guidance
			• root cause analysis or post-mortem procedures • identification of lessons learned and any 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: • actions to be taken in case of an information security event (e.g., noting all relevant details immediately such as malfunction occurring 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 that 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 if the customers within health sector are being affected, CERT NZ, 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 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 at a minimum of: • containment, if the consequences of the incident can spread, so will the systems affected by the incident • 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 form)

Functional Process	Control Area	Requirement	Guidance
			• 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 customers, and 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 the incident resolution process are to be isolated, treated with caution and reported to respective professional bodies. **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 to the response process.
Identify	Roles and Responsibilities	HSUP21: 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 pertaining to the customer environment or services that are being provided to customers including administration, documentation, detection, triage, prioritisation, analysis, communication and coordinating interested parties • an incident response process, to provide the organisation with capability for assessing, responding to, and learning from incidents • only allow 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 to be 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 is to be performed by internal teams, customers, suppliers, and other relevant stakeholders.

Functional Process	Control Area	Requirement	Guidance
Respond	Collection of evidence	HSUP66: 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 the NZ National Cyber Security Centre (NCSC), CERT NZ, NZ Office of the Privacy Commissioner, Te Whatu Ora (if the customers within health sector are affected), 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 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. Digital evidence can surpass organisational or jurisdictional boundaries. In such cases, it is to be ensured that the organisation 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 information security incident	HSUP65: Organisations report all security incidents and near misses to their senior management or to the Board by a nominated Information Security Officer. All customer-related incidents are to be notified to the customer as per agreed timelines.	**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 • 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, documented procedures, including incident scenarios relating to customer information, and its associated assets

Functional Process	Control Area	Requirement	Guidance
			• identifying incidents (both one-off and recurring) with major impact(s) and their causes, to update the organisation's information security risk assessment, risk register and implementing 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 within the Board or steering committee meetings where the minutes are documented. These meeting minutes are referred as evidence at the time of audits. Incidents affecting organisation's customers within the health sector are to be reported to Te Whatu Ora, where applicable, to the NZ's National Cyber Security Centre (NCSC), CERT NZ and the NZ 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 that: • information and its associated assets are protected during disruption • information and operations, as applicable are restored at the required level and in the agreed timeframes.			
Plan	Information security during disruption	HSUP08: Organisations have a documented, approved, business continuity and disaster recovery management, operational resilience policies and procedures in place.	**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, 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 contain the importance of maintaining information security of information, the services that are being provided at an appropriate level during disruption. While developing, implementing, maintaining, and reviewing business continuity and disaster recovery plans, organisations are to consider: • identifying the processes, systems, information, and other relevant equipment that are critical to the delivery of its services • that the 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 and services to its customers the organisation is willing to lose during a disruption (Recovery Point Objective – RPO) • information security controls, supporting systems and tools (as necessary) • processes to maintain existing information security controls during disruption, supporting systems and tools (as necessary) • the compensating controls for security of information that cannot be maintained during disruption (including physical and environmental factors/threats such as, fires, 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 to the delivery of services to customers • 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 loss or

Functional Process	Control Area	Requirement	Guidance
			degradation (including confidentiality, integrity and availability) of the critical systems and services affecting their business operations along with the services that are being provided to their customers. The business continuity and disaster recovery plans are to be tested, reviewed periodically (at least annually or when there are significant changes affecting information or the services that are being provided) so that they are current, available, and accessible to personnel as needed. It is important for organisations to include crisis management planning for the services that are being provided to their customers within the health sector. While managing business continuity, where ICT continuity plays a key part, consider the following requirements to maintain minimal disruption: • regardless of the event, how will the organisation respond and recover from the disruption to the 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 their customers. It is recommended to have communication channels established in the event of disruption or failure 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	HSUP22: Establish criteria for developing business continuity, disaster recovery, operational resilience strategies, and capabilities based on disruption and impact to the organisation.	**Business impact analysis (BIA)** A BIA is performed to determine the IT readiness and security requirements that are to be maintained in the event of failure or disruption. As part of a 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 the organisation's services to their customers within the health sector. Based on the type of impact, the services that are being provided to the customers are to be identified, prioritised and RTO is be assigned (along with resources including IT services, and 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 customers within health sector during disruption. When performing a BIA, 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 customer 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.

Functional Process	Control Area	Requirement	Guidance
			Once a BIA is performed, the results are used to document the continuity plans along with: • business, ICT continuity requirements and objectives including performance and capacity specifications • RTO and RPO for all prioritised services for restoration • RPO of the prioritised IT resources defined as information required for delivery of services to customers and the procedures for its restoration. 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 or contractual agreements. 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 organisational 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 adherence of 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. This documentation supporting the continuity of services is to include: • solution architecture diagrams • administrator and user guides • backup and restoration procedures • software bill of materials (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	HSUP31: 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 and customer's requirements are identified for its redundancy and implemented at an architecture level. The documented and maintained architecture documentation 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:

Functional Process	Control Area	Requirement	Guidance
			• 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 • customer information – offline, backed up customer information and services are tested periodically for restoration purposes and the results documented to ensure data can be restored successfully within agreed timeframes. Implementation of redundancies could introduce risks to maintain integrity of information, and the services that are being provided 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	HSUP56: 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 services. 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, NZ Office of the Privacy Commissioner, etc. These exercises or tests are usually performed on non-production environment(s) such that the customer is not affected. It is important to note that the business continuity plans are different from disaster recovery plans. A failover and failback disaster recovery (DR) exercise is to be conducted annually for critical services and systems. Organisations are to remain cognisant of the role that their information systems and the types of services which they provide to its customers play a vital role in providing continuous business operations (including patient care for their customers within health sector).

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	HSUP32: Rules for effective use of cryptography, including encryption, and key management are defined and implemented.	**Cryptography** Implementation of cryptographic mechanisms ensures that information and the services that are being provided is not altered during transit between the sender and the recipient and while in storage by an unauthorised person or entity. Information and relevant services that are being provided to the customer are to be secured during its transmission as per legal, regulatory, and contractual requirements to protect from malicious parties. This could be achieved by using encryption algorithms, such as transport layer security (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 and the services that are being provided by the organisation to its customers when it is either being stored or transmitted. • integrity or authenticity of information: message authentication codes (MAC) or digital signatures could be used to verify the authenticity or integrity of information that is stored or transmitted along with the services that are being provided. 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: • defined cryptography or encryption procedures (or guidelines) to protect information and the services that are being provided to minimise the risk of not using cryptographic techniques (including inappropriate or incorrect use) is minimised • the required level of protection for information and relevant services (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) • the organisation's 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 customers and applicable external suppliers for encryption services (e.g., with a certification authority) including use of symmetric keys (for data-at-rest) or asymmetric keys.

Functional Process	Control Area	Requirement	Guidance
			Key management plan The 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: • description of the system or service (including the environment), cryptographic system topology (including data flows), use and ownership of keys, key algorithm, key length, key lifetime • roles and administrative responsibilities (whether the keys are managed in-house via a hardware security module (HSM) or by the customer or if outsourced or automatically updated by other suppliers) including the responsibilities of a record keeper and how authorised users obtain access • administrative tasks which are to securely generate, exchange, store, rotate, temporarily/permanently suspended, lost, corrupted, revoked, expired, compromised, or destroyed encryption keys (along with their backup and archival procedures) • information security incident ready set 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 certificates 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 a 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 used for key management (including destroying encryption keys as required) • mitigation strategies to accommodate the risks if keys are owned by customer or supplier, or if they were to be distributed to their intended customers 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 information security and the services that are being provided to customers. 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 that: • individuals and systems accessing the organisation's information and devices that provide such access is to be uniquely identified • individuals and systems are to be authenticated and circumventing the authentication process is prevented • access to customer information and associated assets is to be defined and authorised according to the business and security requirements.			
Plan	Access control	HSUP09: 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, customer and security requirements of the related information assets, including the personnel who will be having 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, (customer as applicable) 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, customer, 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), 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. It is important for organisations to consider latency and response-time in their SLAs for the services offered to its customers. 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 are to be documented for reference purposes.

Functional Process	Control Area	Requirement	Guidance

Protect	Identity Management	HSUP33: 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 their respective devices, services, etc., 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 accounts:
			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 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(s):
			an account that allows access when other privileged accounts do not authenticate. This account bypasses normal controls and so its credentials are stored offline.
			
			All user accounts are to be provided access to systems containing information and relevant services as per documented business, customer 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' identifications, e.g., first name, last name).
			
			If there is no business use for any type of account, or if the user leaves the organisation, it is recommended to disable their access within appropriate time periods, with reviews performed periodically to note that the right access is being provided to the user.

Functional Process	Control Area	Requirement	Guidance
			For internal or supplier managed systems or services, a zero-trust architecture 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 requester's manager and approved by the system or business owner (i.e., to confirm the business requirement) before access is granted. Separate approval process 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, customer 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. For the customers within health sector, it is important to note that though 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	HSUP34: User accounts are authenticated and circumventing the authentication process is prevented.	Organisations processing, storing, or managing information, services, and associated assets are to ensure that their information systems, associated services, and network resources are protected by permitting only authenticated users or processes to gain access to their protected resources. Organisations are to protect the authentication information and process throughout all stages of the information lifecycle. 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. **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) • what you have (e.g., device or security key) • what you are (e.g., fingerprint or your face)

Functional Process	Control Area	Requirement	Guidance
			• where you are (e.g., geolocation or IP-based) • which device or operating system is being used (e.g., organisation issued devices are only 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). Passwords are used in many authentication scenarios and have a limited ability to protect customer information, services, 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 the use of multi-factor authentication (MFA) for all user accounts and especially those with heightened privileges and/or 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 • 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 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, customer 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 to a system or the network (e.g., lost authenticators may be retrieved by an unauthorised person or blocking access to personnel

Functional Process	Control Area	Requirement	Guidance
			who is known to demonstrate malicious activity). Accounts can be prevented from authenticating through several mechanisms: • revocation or replacement of keys, authentication information • disabling or removing the account.

Protect	Access Rights	HSUP35: Access to information and its associated assets is defined and authorised according to the business, customer, and security requirements by adhering to the organisation's identity and access management policy or procedures.	**Provision of access**
			The services and applications used by organisations to support their customers are to 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 and access is activated only after authorisation by the right personnel
			  • the raised request is authorised by requester's manager, then approved by the system or business owner of the information and/or assets considering business, customer, and security requirements
			  • segregation of duties (for approval, implementation and 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 the personnel who had changed their roles within the organisation and the customer organisation
			  • access provided is removed when someone no longer needs access to information and assets especially when they exit from the organisation or customer organisation
			  • temporary access is provided for a limited duration 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.
			
			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

Functional Process	Control Area	Requirement	Guidance
			• as and when there is any change with personnel's role within the same or customer organisation (e.g., job change, promotion, demotion, decommissioning a supplier) or resignation, or termination of employment.
Protect	Privileged Access Rights	HSUP36: 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, the services that are being provided to customers, 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 have access with heightened permissions or privileged access, and this authorisation process follows organisation's identity and access management policy or procedures. While providing privileged access rights, consider: • personnel are trained prior to being given access to system(s) and devices • access is provided only after the requests are authorised; once business, customer, 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 are 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. Especially while accessing customer information, it is important to note that access is restricted to only authorised users. When removing user access, ensure that users who have left the organisation and customer's organisation have their user roles and accounts disabled and/or deleted from the system.

Functional Process	Control Area	Requirement	Guidance
Protect	Access to source code	HSUP37: 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 privileged 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 available to manage and maintain access to these repositories • access is provided based on the business, security and customer requirements along with the roles and responsibilities • 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 supplier environment.

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	HSUP10: The organisation's Board or information security steering committee is accountable for 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 services for their customers. The main objective of the governance is to ensure that the security strategies are aligned with the business and customer objectives of the organisation and are consistent with the regulations, needs and expectations of interested parties. The organisation 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: • the 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 to comply with the overall business and information security requirements are being conducted • annual internal and external audits of the security program are conducted and reported. The results are discussed, 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 including customers are identified, documented, regularly reviewed and the risk owners accept the risks for their systems and authorise or deny the identified risks

Functional Process	Control Area	Requirement	Guidance
			• assignment of security risks to respective business owners to manage the risks in the future • 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	HSUP23: Roles and responsibilities are defined and documented for planning, implementing, operating, assessing, and reporting on the organisation's information security requirements.	Organisational personnel are to understand their role in cyber security governance and resilience. Limited resource availability could make the responsibilities of cyber security fall upon limited personnel. 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 for organisational and customer operations
			• endorse the organisation's security policies along with their updates
			• assesses 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.

Functional Process	Control Area	Requirement	Guidance
			If the management is part of the Board (or steering committee), it is important to note that segregation of duties is to be maintained. **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 the security team • works with finance, legal, human resources, physical security, and 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 evaluate organisational cultural security behaviour and its potential impact on business, security and customer operations • 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 initiatives. • reports to the Board 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, customer 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 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.

Functional Process	Control Area	Requirement	Guidance
			Information Security Manager (ISM) The ISM role focuses on the delivery and operational management of cyber security along with the following responsibilities: • managing and coordinating the response to cyber security incidents, emerging threats and vulnerabilities • developing and maintaining cyber security procedures and guidelines • 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 organisational level for the activities which are to be performed.
Identify	Information security in project management	HSUP24: 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 • project risk management process is factored 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 • information security is part of all phases of project management • 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.

Functional Process	Control Area	Requirement	Guidance
			• performing security due diligence against all components across the project lifecycle considering third-party suppliers (if any). 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 level of possible security. **Security risk assessment (SRA)** A security risk assessment is the process of identifying, evaluating, and prioritising the likelihood of vulnerabilities being exploited along with their impact to various information assets. Performing an SRA helps the organisation to understand its threat landscape and risk profile, business functions, operational processes, information systems and 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 customers, 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 and customer information systems • have better visibility of the information threat landscape. **Security by design** Security by design 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.

Functional Process	Control Area	Requirement	Guidance
Protect	Performance Measurement	HSUP38: 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 including 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? 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 and customer'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 and monitor Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) to assist senior stakeholders in risk, 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's information processing facilities are managed.			

Plan	Policies and Procedures	HSUP11: 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 visitors 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 all 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 services to customers
			• 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 personnel 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 access which is 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 • secured from unauthorised access and 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's 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 organisation's documented processes, up to and including termination of employment, and related civil or criminal penalties.

Functional Process	Control Area	Requirement	Guidance
			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 • stealing the organisation's information assets • gaining unauthorised access to organisational assets in restricted areas which host critical applications or services e.g., server room, network rooms, cabling risers/ducts, uninterruptible power supplies (UPS), generators, building management systems (BMS), heating, ventilation, and air conditioning (HVAC) systems, etc. • ingesting malware into 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 Procedure	HSUP12: A documented and approved procedure to remove papers and removable storage from easily accessible areas is to be implemented.	Documents containing information of customers within the health sector, are often extracted and printed for various purposes. Not everyone working within the organisation are authorised to view or be aware of the information as it might contain personal 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 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 business, customer information is 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 by authorised personnel only 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

Functional Process	Control Area	Requirement	Guidance
			• 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 Care is to be taken within the organisation: • to ensure that the organisation and customer's assets are not left behind (e.g., documents fallen behind drawers or furniture) when facilities are being vacated • visitors are only as close to IT equipment (i.e., servers, storage devices, printers, terminals and displays) as business, customer and security 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 considering health and safety considerations.
Protect	Maintenance of Physical and Environmental Security	HSUP39: 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 processing facilities and assets are to be protected from physical damage, tampering, or unauthorised access including floods, fires, leaks and temperature sensitivities. **Site plan** To determine the different types of threats, one must understand the way the facility is designed. To understand how to protect information 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 security controls implemented to manage the identified risks and their effectiveness • roles and responsibilities of security personnel • administration, operation and maintenance of the access control, security alarm, and utilities installed along with relevant responses 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

Functional Process	Control Area	Requirement	Guidance
			• 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 • 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 premises. This requires relevant teams to understand the weaknesses, potential threats to 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, information 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 and 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.

Functional Process	Control Area	Requirement	Guidance
			In all cases, potential risks arising from cabling incidents or malfunctioning are to be identified and managed.
Protect	Visitor Management System	HSUP40: Secure areas of the organisation are protected from unauthorised personnel.	**Visitor management** A visitor is anyone in an organisation, related facility or in the premise 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 organisational 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., 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 could be provided to visitors, or they could be escorted by the organisation's personnel when they 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 rooms. 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 to be provided to the personnel maintaining the device such as the technical team and reception staff • controls in place to mitigate against potential physical or logical threats

Functional Process	Control Area	Requirement	Guidance
			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 from the standard access cards. 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. **Secure or restricted areas** Organisations might contain secure or restricted areas such as server and/or network room, laboratories, etc. These areas are to be closely monitored and accessed by authorised personnel only. 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, customer, and security requirements. Access reviews are to be performed such that access is provided to authorised personnel only and logs are to be reviewed to check that there is no unauthorised access or tampering. These areas are to be further monitored via surveillance cameras for suspicious behaviour.
Detect	Monitoring of physical and environmental security mechanisms	HSUP57: Installed physical and environmental security mechanisms are monitored for potential security incidents.	**Continuous monitoring** Physical premises and restricted areas 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 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 may go undetected and lead to 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 organisational and customer information is protected when personnel are working from remote locations.			
Protect	Remote Working Requirements	HSUP41: Secure mechanisms are available and supported by a documented policy or guidelines to connect to the organisation's or customer'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 personnel from working from the organisation. For those roles which can be performed from remote locations within the organisation, it is essential to set approved and well documented guidelines for how those roles handle information. **Remote working procedures** Compared to any other field, customers from 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 developing this document, consider: • the use of encryption with multi-factor authentication and conditional access control to login remotely to the organisation's or customer'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 and the services that are being provided • all applications, supporting services and the devices are maintained with latest patch updates • information is not allowed to be downloaded, or stored on personal devices • use of software(s) on all devices to allow the organisation to manage staff devices, enforce security settings and policies such as remote wiping, device location tracking, installation of applications, 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.

Functional Process	Control Area	Requirement	Guidance
			Remote working guidelines • appropriate training and guidance are to be provided to personnel who have been approved to work remotely. • only authorised organisation or customer devices are to be used • the type of customer and organisational information, applications, systems, and services that require authorisation for access are identified • means of connecting securely to the organisation or customer 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 • family and friends are not allowed access to organisation and customer 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	HSUP42: Security controls are implemented if the organisation is developing the web applications to protect them and their customers 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 and 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 services to customers, organisations use or develop various web applications. To protect the information and the services that are being provided 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, 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 may lead to information loss, tampering or unauthorised disclosure. Implementing these measures can: • protect organisations by preventing loss, tampering or unauthorised disclosure of customer and organisation information • protect the organisation from negative legal, financial or reputational exposure • reduce or limit exploitations and injection of malicious code • provide continuous and better experience for customers • help meet the organisation’s customer, 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	HSUP25: 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 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 provided to a customer or 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	HSUP58: Regular reviews are performed to confirm that the legal, regulatory, statutory, and contractual requirements are met.	**Compliance reviews** Compliance reviews help organisations to 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 worst case, loss of patient life (dependent on the services that are being provided to the organisation's customers within health sector) or organisational 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

Functional Process	Control Area	Requirement	Guidance

			• monitor the changes to the laws, regulations, agreements, requirements and determine if they apply to the organisation and/or the customers
			• track the identified changes and prepare an implementation plan so that they are reflected in organisation's documented policies, procedures, guidelines, etc
			• communicate the implemented changes which are being performed to relevant stakeholders.
			
			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 including affected customers in a timely manner.
			
			Planning an audit
			Organisations are to develop and maintain processes to conduct 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, processes, 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 cybersecurity risks against the organisation's strategy, business, and security goals
			  • conducting risk-based cybersecurity assessments against the organisation's technology, people, and processes
			  • assessing the organisation's compliance against cybersecurity regulations, contracts, and other legal and statutory requirements

Functional Process	Control Area	Requirement	Guidance
			• 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. **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)	HSUP13: Organisations have planned maintenance of information and services that are being provided to their customers via cloud services as per documented policies and agreements.	**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 within the CSP's toolset, organisation's requirements and their customers' legal and regulatory obligations.
			
			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
			• whether the cloud service provider:
			  • had undergone a CSA STAR certification and/or attestation
			  • would allow the supplier 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 and customer information
			• policy compliance measurement, exceptions, non-compliance, and continual improvement
			• managing changes to migrate to other cloud service supplier.

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 the 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
			  • 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, its customers and to ensure there is no misunderstanding between the parties.

Identify	Cloud security risk assessment and assurance	HSUP26: 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

Functional Process	Control Area	Requirement	Guidance

			to help them prioritise different risks and develop an appropriate mitigation strategy. A risk assessment matrix usually:
			• identifies the risk profile – strategic, operational, financial, reputational, legal, and external
			• determines the risk criteria – likelihood, impact
			• assess the risks – extreme, high, moderate or medium, low, very low
			• prioritises the risks and implement 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, which could be used to evaluate their own risks.
			
			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 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. While performing 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 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

Functional Process	Control Area	Requirement	Guidance
			• 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. 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 both which are being obtained or offered to their customers through the Cloud Service Provider (CSP) when they are being 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 the 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 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	HSUP43: 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

Functional Process	Control Area	Requirement	Guidance
			• 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 • 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 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 centres or edge locations • Community cloud: is a shared cloud computing service that is targeted to 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 both organisational and customer information.

Functional Process	Control Area	Requirement	Guidance
			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. 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 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)	HSUP44: 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 a organisations internally and to provide its services to its customers 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 integrity, availability and confidentiality (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

Functional Process	Control Area	Requirement	Guidance
			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 • 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	HSUP45: 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 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 helps organisations to: • offer protected services to their customers • meet their service level and operational level agreements • meet legal, statutory, and regulatory requirements • monitor and evaluate the configured cloud services • integrate security-by-design measures to cover cloud supply chain risks • improved compliance practices • share responsibilities and commitment with the CSP

Functional Process	Control Area	Requirement	Guidance
			• 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 in protecting 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 and • maintenance of existing technology services.			
Plan	Security while developing applications, products or services	HSUP14: 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 life cycle so that the controls become an integral part of the organisation's operational capabilities. These are to support the delivery of developed systems including applications, products or services within their risk tolerance to ensure that the 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 apply the principles to every phase of your project 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, customer and security risks. The security engineering principles and the established engineering procedures are to be regularly reviewed to ensure that they are meeting the organisational and customer's security objectives. While developing the security engineering principles, consider: • developing a 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 life cycle to identify potential information security vulnerabilities • documentation of decisions made during the system development life cycle 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 along with 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

Functional Process	Control Area	Requirement	Guidance
			• adoption of zero-trust principle • protection of 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) the written source code to identify errors, i.e., source code review is called source code review. While documenting the standards, for both new changes and enhancements which are being made to the technologies or systems or applications or 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 user 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.

Functional Process	Control Area	Requirement	Guidance
			All developed code is to be tested and monitored for potential vulnerabilities. Identified security vulnerabilities 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. **New acquisitions** Organisations are to document their business, customer, and security requirements while upgrading or acquiring new systems or services or applications and consider: • supporting the organisation's identity mechanisms • protecting and storing audit logs as per business, customer and security requirements • that audit logs are traceable and could be shared to a centralised location for better correlation of events • reporting abnormalities to information access or flow • 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.

Functional Process	Control Area	Requirement	Guidance
Identify	Business, customer and security requirements	HSUP27: Business, customer, and security requirements are identified, documented, and approved when developing or acquiring applications.	**Business, customer 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 of the product • the provider's financial stability and jurisdictional residence • independent third-party assurance reports • risk-based approach that is both user experience and system centric • security functionality • impact on business and security architecture • 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, documentation of the completed evaluation alongside the 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 system is selected, • business, customer (as applicable) 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 the legitimate software may lead to ransomware attacks potentially compromising the organisation's environment. Organisations will need to confirm the source 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., computer equipment), 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 privacy 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

Functional Process	Control Area	Requirement	Guidance
			• 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 that 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 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 • application and database access are to be provided to authorised personnel on a need-to-know basis only • implement additional security mechanisms such as MFA for privileged or administrator accounts • use of approved password managers • collection and retention of information in accordance with regulations and contractual agreements • 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 by 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	HSUP59: 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.

Functional Process	Control Area	Requirement	Guidance
			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, penetration testing, or vulnerability assessment can be used to either identify vulnerabilities or determine the ability of the organisation 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 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 production before rolling out to the production environment. This is to ensure that the introduced system, product or service does not introduce vulnerabilities to the organisation's environment and that the tests are reliable by involving staff and the customer as applicable or 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 business and security requirements. Any services or products that are going to be purchased from a third party are to be evaluated prior to acquiring them. It is important that all the production and non-production environments are monitored by the supplier for potential security vulnerabilities and adequately implement and manage access control. 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	HSUP46: Networks and network devices that are used within the organisation 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 the organisation's network. Tools are usually used to enable real-time network monitoring on endpoint devices and further strengthens 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 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 • performing logging and monitoring activities • logs are being sent to central location for visibility, correlation of events, respond to incidents and overall management • as applicable, configuring 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 • renaming or disabling all default administrative accounts (e.g., root, administrator, etc.). **Zero trust architecture** Organisations are to employ zero trust policy and zero trust architecture where personnel, applications and infrastructure are never trusted and always verified by using strong authentication methods across each application, segmented network and infrastructure components such as routers, switches, cloud, IoT and supply chain. The levels of authorisation are applied based on the business, customer and security requirements. Instead of protecting only the organisation's perimeter, user gets access only when they sign in at work, which does not support the modern need for connectivity and business scalability (e.g., remote work). 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 access is granted at the right level at any given time. **Virtual networks**

Functional Process	Control Area	Requirement	Guidance
			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: • 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	HSUP47: 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, customer domain, wireless access for guests, wireless access for personnel, organisational 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, criticality of information that is being processed at each segregated network domain.

Functional Process	Control Area	Requirement	Guidance
			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) • 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 • as applicable, MAC filtering is to be used. **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 a remote location, e.g., working from home scenarios, implementation of remote access software allows users to connect to the organisation's 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 enable VPN features on their organisation's 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 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 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	HSUP28: Risk assessments are performed on new, existing systems, and applications to understand the risks posed to the organisation while using them.	**Security risk assessment (SRA)** A security risk assessment is the process of identifying, evaluating, and prioritising the likelihood of vulnerabilities being exploited along with their impact to various information assets. Performing an SRA helps the organisation to understand its threat landscape and risk profile, business functions, operational processes, information systems and 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 customers, 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 and customer information systems • have better visibility of the information threat landscape. For suppliers to assess the current and new risks, there is a need to identify the most critical business functions offered to their customers along with their security requirements through performing a business impact analysis (BIA) as defined in business continuity and disaster recovery domain. **Risk assessment methodology** Organisations may take a proactive and repetitive approach to address their internal and customer's information security concerns. A documented risk assessment methodology or processes helps the organisations to: • identify the threats, events, and sources • assess the risks through likelihood and impact • identify and assess the severity of vulnerabilities • manage 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,

Functional Process	Control Area	Requirement	Guidance

			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. A risk assessment matrix usually:
			• identifies the risk profile – strategic, operational, financial, reputational, legal, and external
			• determines the risk criteria – likelihood, impact
			• assess the risks – extreme, high, moderate or medium, low, very low
			• prioritises 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 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. While performing 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, 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

Functional Process	Control Area	Requirement	Guidance
			• 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. 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 the organisation's identified risks and the decision(s) taken by management against each. A simple, consistent format makes it easy for relevant personnel to understand the information as it also contains the likelihood and consequence of a threat occurring, actions along with 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 each risk. While documenting the risks within the risk register, consider: • documenting the risk description including the cause and the outcome (impact on customer, operations, finances, and contracts) • risk status (open/closed/accepted/avoided) • identify the security controls or measures that already in place, the ones needed to be implemented and their effectiveness • risk or business owner to each identified risk • date raised • determining 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, 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

Functional Process	Control Area	Requirement	Guidance
			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 cyber-attack 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** 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. **Control validation plan (CVP)** The CVP outlines the approach or scope of the control validation audit (CVA). This specifies the controls to be audited and the process involved to assess their effectiveness via workshops, interviews, observations, document reviews or configuration reviews. **Control 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 and the services that are being provided is available if it is lost, leaked, or stolen, i.e., information backups • changes to information and the services that are being provided, 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 and the services that are being provided 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	Policy and procedures	HSUP15: A backup and recovery procedure is in place.	**Backup and recovery procedure** Organisations are to establish their own procedures for backing up customer 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., offline 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. The documented procedure is to be periodically reviewed and approved by authorised personnel before being communicated to relevant parties. Any changes identified are to follow the

Functional Process	Control Area	Requirement	Guidance
			organisation’s change management procedures. Exceptions identified are to have a valid business reason, approved and documented for reference.
Protect	Information backup	HSUP48: Backup copies of information, software, services provided, and relevant systems are protected and maintained in accordance with the backup and recovery procedures.	**Backups and recovery** Organisations that provide services to its customers within health sector are to make informed decisions to offer personalised services to their customers. Information backup and recovery are practices of building and storing copies of information to protect them against data loss and to ensure its future availability and integrity. Backup and recovery of information and the services that are being offered to customers are essential for enhancing cyber security, minimise downtimes and to reduce costs in times of crisis. There are also cloud-based tools that offer backup and recovery services along with the ability to tailor the storage needs of organisations and its customers based on the volume of their information. As data theft or loss can have a direct impact on patient care for the customers in health sector, 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 backed up information, stored in at least two locations, one of which is a remote location. Based on the criticality of information, services, and associated assets, backups may be incremental, differential or full. This is to ensure that the information and relevant services can be recovered following a cyber-attack, system failure or loss of storage media. **Backup and recovery plans** Backup and recovery plans are developed and implemented to support the backup and recovery procedures. A backup and recovery plan provides details on what information, its associated assets, and services 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. Also, a backup and recovery plans for information and its associated assets will require: • successful and complete backups to be carried out following documented procedures • backups are generated as per 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

Functional Process	Control Area	Requirement	Guidance
			• automate disaster recovery • data retention is to be kept in a separate dedicated storage environment to where production or backup data is. **Backup retention** There is no one retention requirement for all information which is being collected and maintained within the organisation. The requirements are 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, business, customer and security requirements while retaining information along with the services that are being provided 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	HSUP49: Backups are tested for their restoration in accordance with the documented backup and recovery procedures. Organisations are able to access restored backups as well.	**Backup restoration** Restoration of the information which is already backed up along with the services that are being provided help organisations recover from unplanned events. Backup restoration makes a usable copy of information available to replace lost or corrupted information. It is important to periodically test the backup and recovery plans to ensure that the information is not being corrupted or lost during the process. During restoration, consider: • recovery point objective (RPO), or the amount of loss the organisation considers acceptable in an emergency • recovery time objective (RTO), or organisation’s target for the amount of time 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 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

Functional Process	Control Area	Requirement	Guidance
			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.
Detect	Monitoring of backups	HSUP60: Authorised personnel or teams are alerted upon unsuccessful 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 or 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	Policy and procedures	HSUP16: A documented process is in place for performing changes to new and existing systems or services.	**Change management process** Change management is an organised, formal, and structured approach with processes or mechanisms that enable organisations to transform workflows seamlessly. This also helps in reducing potential business and security risks to the organisation and its customers. 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 and the services that are being provided by the organisation. 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 CAB 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

Functional Process	Control Area	Requirement	Guidance
			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 • 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 their customers, 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 the 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

Functional Process	Control Area	Requirement	Guidance
			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. **Emergency or unplanned changes** These changes are those that need to be made to resolve major incidents which may pose severe risks to the organisation. 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	HSUP29: The proposed changes are to be analysed for potential security threats and their impact on the organisation and their customers.	**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 cyber-attack 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.

Functional Process	Control Area	Requirement	Guidance
			Vulnerability assessments are performed to identify the existing known or potential weaknesses, vulnerabilities within the organisation. 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	HSUP50: Organisations developing inhouse systems, applications, or services are to maintain separate production and non-production environments.	**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 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 organisational personnel and/or customers can access or interact with. While considering multiple environments, 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 having separate domains and have strong authentication procedures in place depending on the criticality of information

Functional Process	Control Area	Requirement	Guidance
			• testing is to be limited to the non-production environments unless a formal change request to the contrary has been approved • production and non-production environments are clearly identified • all environments, including the tools being used are to be updated with latest security patches as per organisation's documented patch management policy or process • secure configuration of applications or systems • any changes being performed are to follow documented and approved 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 a few scenarios (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.
Patch and vulnerability management			
Plan	Policies and procedures	HSUP17: There is a documented and approved process 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 on devices (including printers), where information and the services that are being provided is stored, processed, or used for transmission. This is to reduce the possibility of a potential cyber-attack. The responsibility of patch management lies within the technology team of the organisation 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 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-attack. These practices provide an overview of an organisation's security posture, and the areas that are at most risk, to help prioritise security remediations. Vulnerability scanning tools, where possible are used to identify the vulnerabilities and determine if they are resolved. **Patch and vulnerability management process** Patch and vulnerability management are the first line of defence to remediate vulnerabilities. The documented process defines 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, customer 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 or service or application or product owners

Functional Process	Control Area	Requirement	Guidance
			• 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 is to be determined, reviewed and updated based on the roles and responsibilities within the organisation • the identified vulnerabilities along with patch updates are to be measured and reported to the Board • any exceptions identified from the patch cycle or address a known vulnerability are to obtain a documented approval from authorised personnel; the risks are to be updated in the risk register and compensating controls are implemented to manage the risk • consider auto updates where possible to minimise the possibility of human error. The documented process is to be reviewed along with the other organisational 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 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

Functional Process	Control Area	Requirement	Guidance
			• 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 is usually works in conjunction with the organisation's incident management process. This allows the incident response team to respond effectively to potential incidents which could be raised. If any of these activities are outsourced, the organisation is to obtain service reports from the suppliers to understand the status of their technical environment.
Protect	Patch and vulnerabilities remediation	HSUP51: Identified vulnerabilities or unpatched systems, services or applications are properly identified, tracked, and remediated.	**Unpatched software or known vulnerabilities** Identified unpatched software and known vulnerabilities can be exploited. If there is a patch available for remediation, 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 or unpatched software are to be tracked in the organisation's and customer's risk registers, monitored, and managed till they are resolved. Risks are usually managed by: • implementing the workarounds and/or mitigating strategies as suggested by the authorised sources (e.g., suppliers) after having them approved and authorised by the business owners • disabling the vulnerable services where the risk cannot be accepted • implementing additional firewall rules to restrict the traffic • additional monitoring in place such that there is no unauthorised access to information • enforcing conditional access policies to limit access. If any vulnerability scanning tools are being used, it is important to make sure that these tools are also to be updated with vulnerability signatures and security patches before performing any scans. This ensures that the tool(s) do not violate the organisation's and customer's 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 cloud services are being used to deliver services, it is the responsibility of the cloud service provider to manage the vulnerabilities (i.e., SaaS model). The responsibilities are to be documented within the cloud service agreement along with the processes for reporting and resolving potential vulnerabilities. If there are shared responsibilities between the cloud service provider and the organisation (i.e., IaaS or PaaS model), procedures are to be documented such that the potential or identified vulnerabilities are mitigated and managed.

Functional Process	Control Area	Requirement	Guidance
			Any identified vulnerabilities are to be communicated to potentially affected customers. In all cases, the organisation is ultimately accountable legally by regulations and contractual agreements, and also to their customers in the event any of the identified vulnerabilities get exploited. Hence, it is important to ensure controls and mitigating strategies are always in place to protect the information and the services that are being provided.
Configuration management			
Protect	Secure configuration	HSUP52: Organisations have a standardised baseline configuration in place for new and existing systems, services, and applications.	**Configuration management** For continuous availability of systems and services, organisations will need to have robust, secure, and stable systems that support the information and the services that are being provided to their customers. Configuration management applies to a variety of information systems such as servers, operating systems, networking systems, applications, software, databases, storage systems, and cloud-related services. For systems and services used to manage information, an established configuration management process maintains their consistency and desired state within the organisations. 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 customers • quicker restoration of service if any service is not behaving as expected • identification of all code and configuration deployed into the production environment • effective process to create a duplicate or sandbox environment for any bug fixes • effective change management process to protect system configurations from unauthorised or incorrect changes. Automation tools are often used to maintain configurations based on the needs of the organisation and its customers. 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 the organisation’s documented change management processes. In case of potential incidents, it is easy

Functional Process	Control Area	Requirement	Guidance
			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 organisational and customer 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 to process, store, or transmit information along with the services that are being provided. 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** While developing systems, services or products within the organisation, it is likely that open-source software is used. Care is to be taken such that: • access is restricted to authorised personnel only • only the latest and appropriate releases of the software is used • all activities performed are to be logged, monitored, and investigated for potential security incidents. 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.
Capacity management			
Protect	Capacity management	HSUP53: 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 and providing services to their customers 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 for the customers within the health sector). 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,

Functional Process	Control Area	Requirement	Guidance
			services or applications. It is the responsibility of the system owners to manage this along with the inputs from respective customer, 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, the organisation is 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	HSUP54: 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 the network, services, applications, or operating systems to gain unauthorised access to systems and 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 can be introduced into the systems in the form of email attachments which contain malicious code, via file servers, file sharing software, through remotely exploitable system vulnerabilities. **Protection against malware** A variety of solutions 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 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

Functional Process	Control Area	Requirement	Guidance
			• 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 their 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	HSUP55: 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 and services from unauthorised access is called data leakage prevention. This makes sure that personnel send only the relevant information within and outside of the organisational network. **Tools and technologies** Data loss prevention (DLP) technologies have become essential to protect information and the services that are being offered to its customers by the organisations, 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 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 or customer'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 • while specific roles are authorised to copy or export information to share outside of the 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.

Functional Process	Control Area	Requirement	Guidance
			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 and customer network which allows the monitoring and management of the flow of information via the 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 or customer. The organisation is to consider the following to reduce the risk of data leakage: • classification of information and enforcing 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	HSUP61: The activities performed on the information processing systems, services, and applications are logged and stored as per the organisation's (and the customer's) logging and auditing requirements.	**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: • 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

Functional Process	Control Area	Requirement	Guidance
			• 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: • customer requirements • 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, and reviewed periodically for potential incidents. Logs are to be analysed to confirm the occurrence of an unusual activity or an anomalous behaviour which might have compromised information and the services that are being used within the organisation or offered to its customers. 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 along with its customers, 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 and its customers. This helps to uncover misuse of information and information processing systems. Audit logs are to be stored as per organisation's (and customer'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 • reporting the audit logs which are on/off at any point in time

Functional Process	Control Area	Requirement	Guidance
			• 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 security operation centre (SOC) 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 and the services that are being provided to its customers by filtering and prioritising the alerts which are generated by the software to respond to potential security threats and vulnerabilities before the organisation or their customer'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 organisation and their customer'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	HSUP62: The information processing systems, applications, devices, and services are synchronised to an approved time source.	Different types of end point devices are being used to process, store, or transmit information to provide services within the organisation and to their customers. 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. Un-synchronised clocks on the devices across the organisational 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 protocol 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 to determine 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 access to a health service provider network or the internet.
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.
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.
Botnet	A collection of computers linked together to perform a specific task. They can be misused for malicious purposes to control a health service provider's computer and use it to carry out attacks on devices outside the network.
Break glass account	An account that allows standard controls to be bypassed and should only be used when necessary and under supervision.
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 continuity plan (BCP)	Documented procedures that guide organisations to respond, recover, resume, and restore to a pre-defined level of operation following disruption.

Term	Definition
Business impact analysis (BIA)	A process and corresponding toolset for identifying those cyber assets that are most critical to the accomplishment of an organisation's mission.
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 patient surge.
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 must 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. 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

Term	Definition
	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 (Cloud 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 PII 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, 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.
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

Term	Definition
	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 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

Term	Definition
	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 personnel within the organisation.
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.
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.

Term	Definition
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.
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're looking to use with a public cloud service, find out how important it is to your organisation, the NZ 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	A combination of customer and organisational information.
Hardware security module (HSM)	A dedicated crypto processor that is specifically designed for the protection of the crypto key lifecycle. It manages, processes, and stores cryptographic keys.
Health information	This includes personal health information (PHI), patient identifiable information (PII), and the implementation of general IT controls within the health service provider.
Health information assets	This includes paper based and digitally stored health information, computing devices (e.g., computers, servers, mobile phones), printers, network equipment, specialist medical devices, media storage, that contain health information or support the implementation of general IT controls for a health service provider.
High availability	A failover feature to ensure availability during device or component interruptions.
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.
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

Term	Definition
	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 to various operational, financial, reputational, compliance, and strategic risks.
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

Term	Definition
	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 an 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 management agents, allowing information technology staff to discover, maintain, and control these devices.
Master services 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.

Term	Definition
Memorandum of understanding (MOU)	A memorandum of understanding is often used commercially to establish a partnership with other businesses or commercial entities. Therefore, each MOU will be specific to each potential partnership.
Message authentication code (MAC) address	A unique 48-bit value that is assigned to a particular wireless network interface by the manufacturer.
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-protocol label switching (MPLS)	An IP packet routing technique that routes IP packet through paths via labels instead of looking at complex routing tables of routers. This feature helps in increasing the delivery rate of IP packets.
Multi-tenant 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.
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.

Term	Definition
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.
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.

Term	Definition
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 and web application security.
Organisation	Organisation in this document refers to the supplier organisation to whom this guidance will be applicable to.
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 doesn't 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 identifiable information (PII)	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, retinal 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	Organisational 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.
Privacy impact assessment (PIA)	A tool used by organisations to help them identify and assess the privacy risks arising from the use and handling of PHI and PII. A PIA will also propose ways to mitigate or minimise these risks.
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.
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 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.

Term	Definition
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 should take to restore normal operations following an outage or data loss.
Remediation	Implementing corrective action to eliminate a risk.
Remote Access	Access to an organisational 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).
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 organisational operations (including mission, functions, image, reputation), organisational assets, individuals, other organisations, resulting from the operation of a system.

Term	Definition
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 an 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 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.

Term	Definition
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 must 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.
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.

Term	Definition
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 operations centre (SOC) team	An organisational or business unit operating at the centre of security operations to manage and improve an organisation's overall security posture. Its primary function is to detect, analyse and respond to cybersecurity events, including threats and incidents, employing people, processes and technology. Teams are responsible for managing security infrastructure and configuring and deploying various security solutions, tools and products.
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.
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,

Term	Definition
	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).
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 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.

Term	Definition
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 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 analysis (TVA)	Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.

Term	Definition
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.
Tunnelling	Technology enabling one network to send its data via another network's connections. Tunneling 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 machines (VMs)	It is no different to any other physical computer like a laptop, smart phone, or server. It has a CPU, memory,

Term	Definition
	disks to store organisation files and can connect to the internet if needed. A VM is a computer file or an image that behaves like an actual computer. It can run in a window as a separate computing environment. The VM is partitioned from the rest of the system, meaning that software inside a VM can't interfere with the host computer's primary operating system.
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	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.
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.

Term	Definition
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.
Wireless access point (WAP)	A device that allows wireless devices to connect to a wired network using wi-fi, or related standards.
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.