MINISTRY
OF
SECURITY

ISO 27001:2013

TO

ISO 27001:2022

COMPLETE TRANSITION GUIDE

Introduction

The most awaited ISO/IEC 27001:2022 was published on October 25, 2022. Some of the important updates of ISO/IEC 27001:2022 include - major change of Annex A and minor updates to the clauses.

a) Main Changes in Standard

Details	ISO 27001:2013	ISO 27001:2022
Clauses	11	11
Controls	114	93
Number of Domains in Annexure A	14	4

b) Control Group Domains

Control Group	Count
A.5 Organizational controls	37 controls
A.6 People controls	8 controls
A.7 Physical controls	14 controls
A.8 Technological controls	34 controls

c) Control Group Changes

Control Group	Count
Merged Controls	57 controls
New Controls	11 controls
Deleted Controls	03 controls
Controls with no changes	35 controls

d) Transition Timelines

Transition Details	Timelines
Companies can be certified against 2013 revision	Until 31st October 2023
Companies can be certified against new 2022 revision	From 25th October 2022
Companies certified against the 2013 revision must transition to 2022 revision	By 31st October 2025

Clauses

Clause	Requirement	Transition Details
4.1 Understanding the organization and its context	No Changes	No Changes
4.2 Understanding the needs and expectations of interested parties	The organization shall determine: a) interested parties that are relevant to the information security management system; b) the relevant requirements of these interested parties; c) which of these requirements will be addressed through the information security management system.	**Document to be updated:** ISMS Needs and Expectations of Interested Parties Register **Implementation:** In addition to capturing the requirements of the interested parties, add an additional section to demonstrate how each of the requirements of the interested parties are met through ISMS.
4.3 Determining the scope of the information security management system	No Changes	No Changes
4.4 Information security management system	The organization shall establish, implement, maintain and continually improve an information security management system, including the processes needed and their interactions, in accordance with the requirements of this document.	**Document to be updated:** ISMS Manual **Implementation:** Update the ISMS Manual to reflect how process and interactions are put in place to demonstrate how ISMS shall be implemented and maintained for continual improvement.
5.1 Leadership and commitment	No Changes	No Changes
5.2 Policy	No Changes	No Changes
5.3 Organizational roles, responsibilities and authorities	No Changes	No Changes
6.1 Actions to address risks and opportunities	No Changes	No Changes
6.1.2 Information security risk assessment	No Changes	**Document to be updated:** Risk Assessment Document **Implementation:** Update the risk assessment document with new controls mapped to each risk.
6.1.3 Information security risk treatment	d) produce a Statement of Applicability that contains:	**Document to be updated:** Statement of Applicability

	— the necessary controls (see 6.1.3 b) and c));	**Implementation:** Update the SOA with 93 controls from Annex A.
6.2 Information security objectives and planning to achieve them	The organization shall establish information security objectives at relevant functions and levels. The information security objectives shall: a) be consistent with the information security policy; b) be measurable (if practicable); c) take into account applicable information security requirements, and results from risk assessment and risk treatment; d) be monitored; e) be communicated; f) be updated as appropriate; g) be available as documented information.	**Document to be updated:** 1) Functional Objectives Register 2) ISMS Effectiveness Metrics **Implementation:** 1) Define Information Security Goals 2) Derive Information Security Objectives 3) Define IS objectives mapped to each functional level. 4) Define metrics and process to monitor how each objective will be measured. 5) Update effectiveness metrics for each function and measure them on periodic basis. 6) Document the measurement results.
6.3 Planning of changes	When the organization determines the need for changes to the information security management system, the changes shall be carried out in a planned manner.	**Document to be updated:** ISMS Manual **Implementation:** Establish a process in ISMS Manual to demonstrate how changes to ISMS will be followed. (Ideally Change Management process should be followed)
7.1 Resources	No Changes	No Changes
7.2 Competence	No Changes	No Changes
7.3 Awareness	No Changes	No Changes
7.4 Communication	The organization shall determine the need for internal and external communications relevant to the information security management system including: a) on what to communicate; b) when to communicate; c) with whom to communicate; d) how to communicate	**Document to be updated:** Communication Plan **Implementation:** Previously it was d) who shall communicate; and e) the processes by which communication shall be effected. This section is now updated to d) how to communicate. This means there is no requirement to document who shall be communicating and the processes

		by which communication shall be effected.
7.5 Documented information	No Changes	No Changes
8.1 Operational planning and control	The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Clause 6, by: — establishing criteria for the processes; — implementing control of the processes in accordance with the criteria The organization shall ensure that externally provided processes, products or services that are relevant to the information security management system are controlled.	**Document to be updated:** ISMS Manual **Implementation:** The clause is tweaked to make it more meaningful.
8.2 Information security risk assessment	No Changes	No Changes
8.3 Information security risk treatment	No Changes	No Changes
9.1 Monitoring, measurement, analysis and evaluation	Minor Changes	**Rephrased -** Documented information shall be available as evidence of the results
9.2 Internal audit	9.2.1 General 9.2.2 Internal audit programme	**Document to be updated:** Internal Audit Procedure **Implementation:** Requirements are unchanged but divided into two sub-clauses 9.2.1 - General 9.2.2 - Internal Audit Program
9.3 Management review	9.3.1 General 9.3.2 Management review inputs 9.3.3 Management review results	**Document to be updated:** Management Review Presentation & Minutes of Meeting. **Implementation:** Requirements are largely unchanged but divided into three sub-clauses (Management Review to include changes to "Interested Parties") 9.3.1 - General 9.3.2 - Management Review Inputs 9.3.3. - Management Review Results

		Update the MRM Presentation Inputs Slide to address a new point - if there are any changes in needs and expectations of interested parties that are relevant to the information security management system
10.1 Continual improvement & 10.2 Nonconformity and corrective action	Minor Change	10.1 & 10.2 order is interchanged. In the 2022 version - 10.1 - Continual improvement 10.2 - Nonconformity and corrective action

Controls

a) Merged Controls (57)

Merged Controls	Previous Controls
5.1 Policies for information security	5.1.1 & 5.1.2
5.8 Information security in project management	6.1.5 & 14.1.1
5.9 Inventory of information and other associated assets	8.1.1 & 8.1.2
5.10 Acceptable use of information and other associated assets	8.1.3 & 8.2.3
5.14 Information transfer	13.2.1 & 13.2.2 & 13.2.3
5.15 Access Control	9.1.1 & 9.1.2
5.16 Identity management	9.2.1 & 9.4.3
5.17 Authentication information	9.2.4 & 9.3.1 & 9.4.3
5.18 Access rights	9.2.2 & 9.2.5 & 9.2.6
5.22 Monitoring, review and change management of supplier services	15.2.1 & 15.2.2
5.29 Information security during disruption	17.1.1 & 17.1.2 & 17.1.3
5.31 Legal, statutory, regulatory and contractual requirements	18.1.1 & 18.1.5
5.36 Compliance with policies, rules and standards for information security	18.2.2 & 18.2.3
6.8 Information security event reporting	16.1.2 & 16.1.3
7.2 Physical entry	11.1.2 & 11.1.6
7.10 Storage media	8.3.1 & 8.3.2 & 8.3.3, & 11.2.5
8.1 User end point device	6.2.1 & 11.2.8
8.8 Management of technical vulnerabilities	12.6.1 & 18.2.3
8.15 Logging	12.4.1 & 12.4.2 & 12.4.3
8.19 Installation of software on operational systems	12.5.1 & 12.6.2
8.24 Use of cryptography	10.1.1 & 10.1.2 & 18.1.5
8.26 Application security requirement	14.1.2 & 14.1.3
8.29 Security testing in development and acceptance	14.2.8 & 14.2.9
8.31 Separation of development, test and production environments	12.1.4 & 14.2.6
8.32 Change management	12.1.2 & 14.2.2 & 14.2.3 & 14.2.4

b) Deleted Controls (3)

Deleted Controls		
8.2.3 Handling of Assets	11.2.5 Removal of Assets	16.1.3 Reporting of Information Security Weakness

c) New Controls (11)

Control	Summary of Control
5.7 Threat Intelligence	• Establishing objectives • Identifying, vetting and selecting internal and external information sources • Processing information collected • Analyzing information • Communicating and sharing
5.23 Information Security for use of cloud services	• Should establish and communicate topic-specific policy • Information security requirements • Selection criteria & scope • Roles & responsibilities • Information security capabilities & controls by cloud service providers • Manage multiple cloud services • Incident management • Monitoring, reviewing and evaluating the ongoing use • Exit strategy • Risk assessment associated with cloud service • Agreement requirements
5.30 ICT Readiness for business continuity	• Organizational structure • ICT continuity plans, including response & recovery procedures • Performance & capacity specifications • RTO & RPO
7.4 Physical Security Monitoring	• Guards, intruder alarms, video monitoring etc., • Access restrictions to monitoring systems • Tamper proof. • Testing • Local laws and consider regulations including data protection and PII protection legislation
8.9 Configuration Management	• Define and implement processes and tools to enforce the defined configurations • Roles & Responsibilities • Standard templates • CMDB or configuration templates • Monitoring & review of configurations • Manual or automated corrective actions
8.10 Information Deletion	• Deletion method • Record results as evidence of deletion

	• Third party agreements should consider information deletion clause during termination • Also applicable for cloud service providers
8.11 Data Masking	• Data masking, pseudonymization or anonymization. • Access on need-to-know basis • Data Obfuscation • Obfuscation of obfuscation • Legal or regulatory requirements (e.g.: PCI)
8.12 Data Leakage Prevention	• Data identification & classification • Monitor channels • Acting to prevent information from leaking
8.16 Monitoring Services	• Monitoring Scope • Monitoring Sources • Baselines • Monitoring System Configuration • Monitoring Tools
8.22 Web Filtering	• Block IP or domains concerned • Acceptable usage policy • Training on appropriate use of online resources
8.28 Secure Coding	• Establish and apply minimum secure baselines • Approved principles for secure coding • Secure coding practices • Prohibit insecure design techniques • Static application security testing • Protect source code from unauthorized access • Updates should be securely packaged and deployed • Security of external tools and libraries

Detailed Implementation Steps

Controls	Transition Details
5.7 Threat Intelligence	**Control Statement:** Information relating to information security threats should be collected and analyzed to produce threat Intelligence. **Document:** Threat Intelligence Policy (Optional) **Description :** This control requires the organisation to gather information about threats and analyze them, in order to take appropriate mitigation actions. This information could be about particular attacks, about methods and technologies the attackers are using, and/or about attack trends. The organisation should gather this information internally, as well as from external sources like vendor reports, government agency announcements, etc. **Process :** The organisation can set the processes for how to gather and use the threat information to introduce preventive controls in organisation IT systems, to improve the risk assessment, and to introduce new methods for security testing. **Implementation:** Define a process to demonstrate a) How Information about existing or emerging threats is collected and analyzed. (Ex: independent providers or advisors, government agencies or collaborative threat intelligence groups.) b) Threat intelligence should be considered at all the three layers a) strategic threat intelligence: exchange of high-level information about the changing threat landscape (e.g. types of attackers or types of attacks); b) tactical threat intelligence: information about attacker methodologies, tools and technologies involved; c) Operational threat intelligence: details about specific attacks, including technical indicators. c) Threat intelligence should be relevant, insightful, contextual, actionable. d) Threat Intelligence Policy and implementation should clearly mention the process involved in identifying, vetting and selecting internal and external information sources, how they are processed and communicated to relevant stakeholders. e) Where feasible, incorporate the information gathered from threat intelligence into organization risk management process, as additional input to technical preventive and detective controls like firewalls, intrusion detection system, or anti malware solutions and information security test processes and techniques.

5.23 Information Security for use of cloud services	**Control Statement:** Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organization's information security requirements. **Document:** Cloud Services Policy (Optional) **Description:** This control requires organisation to set security requirements for cloud services in order to save better protection of organisation information in the cloud. This includes purchasing, using, managing, and terminating the use of cloud services. **Process:** Organisation should set up a process to determine security requirements for cloud services and for determining the criteria for selecting a cloud provider; further, organisation should define a process for determining acceptable use of the cloud, and also the security requirements when cancelling the use of a cloud service. **Implementation:** **Cloud Service Policy & Process** The organization shall define a policy and process to demonstrate a) use of Cloud Services b) To manage information security risks with the use of cloud services. c) Shared Roles & Responsibilities of both organization (cloud customer) and cloud service provider. d) information security requirements associated with the use of the cloud services; e) cloud service selection criteria and scope of cloud service usage; f) which information security controls are managed by the cloud service provider and which are managed by the organization as the cloud service customer; g) how to obtain assurance on information security controls implemented by cloud service providers; h) how to manage controls, interfaces and changes in services when an organization uses multiple cloud services, particularly from different cloud service providers; i) procedures for handling information security incidents in relation to the use of cloud services; j) approach for monitoring, reviewing and evaluating the ongoing use of cloud services to manage information security risks; k) how to change or stop the use of cloud services including exit strategies for cloud services. **Cloud Service Agreement**

	a) A cloud service agreement should address the CIA and information handling requirements of the organization, with appropriate cloud service level objectives and cloud service qualitative objectives. b) Also undertake relevant risk assessments to identify the risks associated with using the cloud service. Any residual risks connected to the use of the cloud service should be clearly identified and accepted by the management of the organization. The contract should clearly define c) providing solutions based on industry accepted standards for architecture and infrastructure; d) managing access controls of the cloud service to meet the requirements of the organization; e) implementing malware monitoring and protection solutions; f) processing and storing the organization's sensitive information in approved locations (e.g. particular country or region) or within or subject to a particular jurisdiction; g) providing dedicated support in the event of an information security incident in the cloud service environment; h) ensuring that the organization's information security requirements are met in the event of cloud services being further sub-contracted to an external supplier (or prohibiting cloud services from being sub-contracted); i) supporting the organization in gathering digital evidence, taking into consideration laws and regulations for digital evidence across different jurisdictions; j) providing appropriate support and availability of services for an appropriate time frame when the organization wants to exit from the cloud service; k) providing required backup of data and configuration information and securely managing backups as applicable, based on the capabilities of the cloud service provider used by the organization, acting as the cloud service customer; l) providing and returning information such as configuration files, source code and data that are owned by the organization, acting as the cloud service customer, when requested during the service provision or at termination of service. **Changes to Cloud Infrastructure** The organization, acting as the cloud service customer, should consider whether the agreement should require cloud service providers to provide advance notification prior to any substantive customer impacting changes being made to the way the service is delivered to the organization, including:

	a) changes to the technical infrastructure (e.g. relocation, reconfiguration, or changes in hardware/software) that affect or change the cloud service offering; b) processing or storing information in a new geographical or legal jurisdiction; c) use of peer cloud service providers or other sub-contractors (including changing existing or using new parties). **Cloud Service Communication** a) Both the Cloud customer and cloud service providers should maintain close contact to enable mutual exchange of information b) A mechanism should be setup, to monitor each service characteristic and report failures to the commitments contained in the agreements.
5.30 ICT Readiness for business continuity	**Control Statement:** ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements. **Policy:** ICT readiness for business continuity (Optional) **Description :** This control requires organisationr information and communication technology to be ready for potential disruptions so that required information and assets are available when needed. This includes readiness planning, implementation, maintenance, and testing. **Process:** The organisation should also set up the maintenance process for technology, and the testing process for disaster recovery and/or business continuity plans. **Implementation:** The organization shall a) Perform business impact analysis (BIA) to determine ICT continuity requirements. b) BIA process should use impact types and criteria to assess the impacts resulting from the disruption of business activities c) The magnitude and duration of the resulting impact should be used to identify prioritized activities which should be assigned a recovery time objective (RTO). d) Ensure the BIA determines which resources are needed to support prioritized activities. e) Based on the outputs from the BIA and risk assessment involving ICT services, the organization should identify and select ICT continuity strategies that consider options for before, during and after disruption. f) Based on the strategies, plans should be developed, implemented and tested to meet the required availability level of ICT services and in the required time frames following interruption to, or failure of, critical processes.

<table>
<tr>
<td></td>
<td>
g) ICT continuity plans, including response and recovery procedures detailing how the organization is planning to manage an ICT service disruption, are regularly evaluated through exercises and tests and approved by management;
h) ICT continuity plans include the following ICT continuity information:
1. performance and capacity specifications to meet the business continuity requirements and objectives as specified in the BIA;
2. RTO of each prioritized ICT service and the procedures for restoring those components;
3. RPO of the prioritized ICT resources defined as information and the procedures for restoring the information.
i) an adequate organizational structure is in place to prepare for, mitigate and respond to a disruption supported by personnel with the necessary responsibility, authority and competence;
</td>
</tr>
<tr>
<td><b>7.4 Physical Security Monitoring</b></td>
<td>
<b>Control Statement:</b>
Premises should be continuously monitored for unauthorized physical access
<b>Documentation:</b> Physical Security Policy
<b>Description :</b>
This control requires organisation to monitor sensitive areas in order to enable only authorized people to access them. This might include offices, production facilities, warehouses, and other premises.
<b>Process:</b>
The organisation should define process for who is in charge of the monitoring of sensitive areas, what communication channels to use to report an incident.
<b>Implementation:</b>
Physical premises shall be continuously monitored to detect unauthorized access or suspicious behavior by surveillance systems,
<table>
<tr><td>• Guards</td><td>• Contact Detector</td></tr>
<tr><td>• CCTV</td><td>• Panic Alarm</td></tr>
<tr><td>• Sound/Motion Detector alarm</td><td>• Physical security information management software managed internally or by a monitoring service provider.</td></tr>
</table>
a) Monitoring systems should be protected from unauthorized access
b) The control panel and the detectors should have tamper proof mechanisms.
c) The systems should regularly be tested.
d) Any monitoring and recording mechanism should be used taking into consideration local laws and regulations including data protection and PII protection legislation, especially regarding the monitoring of personnel and recorded video retention periods.
</td>
</tr>
</table>

8.9 Configuration Management	**Control Statement:** Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed. **Document :** Configuration Management Policy **Description:** This control requires organisation to manage the whole cycle of security configuration for organisation technology to ensure a proper level of security and to avoid any unauthorized changes. This includes configuration definition, implementation, monitoring, and review. **Process:** Organisation should set up a process for proposing, reviewing, and approving security configurations, as well as the processes for managing and monitoring the configurations. **Implementation :** <u>General</u> a) The organization should define and implement processes and tools to enforce the defined configurations (including security configurations) for hardware, software, services (e.g. cloud services) and networks, for newly installed systems as well as for operational systems over their lifetime. b) Roles, responsibilities and procedures should be defined w.r.t to configuration changes. c) Use of Standard templates for the secure configuration of hardware, software, services and networks should be defined. d) The templates should be reviewed periodically and updated when new threats or vulnerabilities need to be addressed, or when new software or hardware versions are introduced. e) Changes to configurations should follow the change management process. f) Configuration records can contain as relevant: 1. up-to-date owner or point of contact information for the asset; 2. date of the last change of configuration; 3. version of configuration template; 4. relation to configurations of other assets. g) Configurations should be monitored with a comprehensive set of system management tools and should be reviewed on a regular basis to verify configuration settings, evaluate password strengths and assess activities performed.

8.10 Information Deletion

Control Statement:

Information stored in information systems, devices or in any other storage media should be deleted when no longer required.

Documentation: Information Disposal Policy

Description:

This control requires organisation to delete data when no longer required, in order to avoid leakage of sensitive information and to enable compliance with privacy and other requirements. This could include deletion in organisation IT systems, removable media, or cloud services.

Process: Organisation should set up a process that will define which data need to be deleted and when, and define responsibilities and methods for deletion.

Implementation:

a) Sensitive information should not be kept for longer than required

b) When deleting information on systems, applications and services, the following should be considered:

   1. selecting a deletion method (e.g. electronic overwriting or cryptographic erasure) in accordance with business requirements and taking into consideration relevant laws and regulations;
   2. recording the results of deletion as evidence;
   3. when using service suppliers of information deletion, obtaining evidence of information deletion from them.

c) Where third parties store the organization's information on its behalf, the organization should consider the inclusion of requirements on information deletion into the third-party agreements to enforce it during and upon termination of such services.

Deletion methods

d) Sensitive information should be deleted when no longer required, by:

   1. configuring systems to securely destroy information when no longer required (e.g. after a defined period subject to the topic-specific policy on data retention or by subject access request);
   2. deleting obsolete versions, copies and temporary files.
   3. using approved, secure deletion software to permanently delete information.
   4. using approved, certified providers of secure disposal services;
   5. using disposal mechanisms appropriate for the type of storage media being disposed of (e.g. degaussing hard disk drives)

e) The organization should verify if the deletion method provided by the cloud service provider is acceptable or not.

f) To avoid the unintentional exposure of sensitive information when equipment is being sent back to vendors, sensitive information should be protected by removing auxiliary storages (e.g. hard disk drives) and memory before equipment leaves the organization's premises.

8.11 Data Masking

Control Statement:

Data masking should be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.

Documentation: Information Protection Policy (Optional)

Description:

This control requires organisation to use data masking together with access control in order to limit the exposure of sensitive information. This primarily means personal data, because they are heavily regulated through privacy regulations, but it could also include other categories of sensitive data.

Processes:

Organisation should set up processes that will determine which data need to be masked, who can access which type of data, and which methods will be used to mask the data.

Implementation:

a) Organization should consider hiding sensitive data by using techniques such as data masking, pseudonymization or anonymization.

b) When using such techniques, it should be verified that data has been adequately pseudonymized or anonymized.

c) Additional techniques for data masking include:

1. encryption (requiring authorized users to have a key);
2. nulling or deleting characters (preventing unauthorized users from seeing full messages);
3. varying numbers and dates;
4. substitution (changing one value for another to hide sensitive data);
5. replacing values with their hash.

d) The following should be considered when implementing data masking techniques:

1. not granting all users access to all data.
2. Use of obfuscated data in certain cases.
3. any legal or regulatory requirements

e) The following should be considered when using data masking, pseudonymization or anonymization:

1. level of strength of data masking, pseudonymization or anonymization according to the usage of the processed data;
2. access controls to the processed data;
3. agreements or restrictions on usage of the processed data;
4. prohibiting collating the processed data with other information in order to identify the PII principal;
5. keeping track of providing and receiving the processed data.

8.12 Data Leakage Prevention	**Control Statement:** Data leakage prevention measures should be applied to systems, networks and any other devices that process, store or transmit sensitive information. **Documentation:** Information Protection Policy (Optional) **Description:** This control requires organisation to apply various data leakage measures in order to avoid unauthorized disclosure of sensitive information, and if such incidents happen, to detect them in a timely manner. This includes information in IT systems, networks, or any devices. **Processes:** Organisation should set up processes that determine the sensitivity of data, assess the risks of various technologies (e.g., risks of taking photos of sensitive information with a smartphone), monitor channels with the potential of data leakage, and define which technology to use to block the exposure of sensitive data. **Implementation:** a) The organization should consider the following 1. identifying and classifying information to protect against leakage 2. monitoring channels of data leakage 3. acting to prevent information from leaking b) Data leakage prevention tools should be used to: 1. identify and monitor sensitive information at risk 2. detect the disclosure of sensitive information 3. block user actions or network transmissions that expose sensitive information c) The organization should determine if it is necessary to restrict a user's ability to copy and paste or upload data to services, devices and storage media outside of the organization. d) If data export is required, the data owner should be allowed to approve the export and hold users accountable for their actions. e) Taking screenshots or photographs of the screen should be addressed through terms and conditions of use, training and auditing. f) Where data is backed up, care should be taken to ensure sensitive information is protected using measures such as encryption, access control and physical protection of the storage media holding the backup. g) Data leakage prevention should also be considered to protect against the intelligence actions of an adversary from obtaining confidential or secret information (geopolitical, human, financial, commercial, scientific or any other) which can be of interest for espionage or can be critical for the community.

8.16 Monitoring Services	**Control Statement:** Networks, systems and applications should be monitored for anomalous behavior and appropriate actions taken to evaluate potential information security incidents. **Documentation:** Logging & Monitoring Policy **Description:** This control requires organisation to monitor organisation systems in order to recognize unusual activities and, if needed, to activate the appropriate incident response. This includes monitoring of organisation IT systems, networks, and applications. **Processes:** Organisation should set up a process that defines which systems will be monitored; how the responsibilities for monitoring are determined; and the methods of monitoring, establishing a baseline for unusual activities, and reporting events and incidents. **Implementation:** a) The monitoring scope and level should be aligned with business and information security requirements and relevant laws and regulations. b) Monitoring records should be maintained for defined retention periods. c) The following should be considered for inclusion within the monitoring system: 1. outbound and inbound network, system and application traffic; 2. access to systems, servers, networking equipment, monitoring system, critical applications, etc.; 3. critical or admin level system and network configuration files; logs from security tools [e.g. antivirus, IDS, intrusion prevention system (IPS), web filters, firewalls, data leakage prevention]; 4. event logs relating to system and network activity; 5. checking that the code being executed is authorized to run in the system and that it has not been tampered with (e.g. by recompilation to add additional unwanted code); 6. use of the resources (e.g. CPU, hard disks, memory, bandwidth) and their performance. d) The organization should establish a baseline of normal behavior and monitor against this baseline for anomalies. e) When establishing a baseline, the following should be considered: 1. reviewing utilization of systems at normal and peak periods; 2. usual time of access, location of access, frequency of access for each user or group of users. f) The monitoring system should be configured against the established baseline to identify anomalous behavior, such as: 1. unplanned termination of processes or applications;

	2. activity typically associated with malware or traffic originating from known malicious IP addresses or network domains 3. known attack characteristics (e.g. DoS and buffer overflows); 4. unusual system behavior (e.g. keystroke logging, process injection and deviations in use of standard protocols); 5. bottlenecks and overloads (e.g. network queuing, latency levels and network jitter); 6. unauthorized access (actual or attempted) to systems or information; 7. unauthorized scanning of business applications, systems and networks; 8. successful and unsuccessful attempts to access protected resources (e.g. DNS servers, web portals and file systems); 9. unusual user and system behavior in relation to expected behavior. g) Continuous Monitoring should be done in real time or in periodic intervals, subject to organizational need and capabilities. h) Monitoring tools should include 1. the ability to handle large amounts of data, adapt to a constantly changing threat landscape, and allow for real-time notification. 2. be able to recognize specific signatures and data or network or application behavior patterns. i) Automated monitoring software should be configured to generate alerts based on predefined thresholds. j) The alerting system should be tuned and trained on the organization's baseline to minimize false positives. k) Personnel should be dedicated to respond to alerts and should be properly trained to accurately interpret potential incidents. l) There should be redundant systems and processes in place to receive and respond to alert notifications. m) Abnormal events should be communicated to relevant parties in order to improve the following activities: auditing, security evaluation, vulnerability scanning and monitoring. n) Procedures should be in place to respond to positive indicators from the monitoring system in a timely manner, in order to minimize the effect of adverse events on information security. o) Procedures should also be established to identify and address false positives including tuning the monitoring software to reduce the number of future false positives.

8.23 Web Filtering	**Control Statement:** Access to external websites should be managed to reduce exposure to malicious content **Documentation:** Network Security Policy (Optional) **Description:** This control requires organisation to manage which websites organisation users are accessing, in order to protect organisation IT systems. This way, organisation can prevent organisation systems from being compromised by malicious code, and also prevent users from using illegal materials from the Internet. **Processes:** Organisation should set up processes that determine which types of websites are not allowed, and how the web filtering tools are maintained. **Implementation:** a) The organization should reduce the risks of its personnel accessing websites that contain illegal information or are known to contain viruses or phishing material by blocking the IP address or domain of the website(s) concerned. b) The organization should identify the types of websites to which personnel should or should not have access. c) The organization should establish rules for safe and appropriate use of online resources, including any restriction to undesirable or inappropriate websites and web-based applications. d) Training should be given to personnel on the secure and appropriate use of online resources including access to the web. e) The training should include the organization's rules, contact point for raising security concerns, and exception process when restricted web resources need to be accessed for legitimate business reasons. f) Training should also be given to personnel to ensure that they do not overrule any browser advisory that reports that a website is not secure but allows the user to proceed.
8.28 Secure Coding	**Control Statement:** Secure coding principles should be applied to software development. **Documentation:** Secure Development Policy **Description:** This control requires organisation to establish secure coding principles and apply them to organisation software development in order to reduce security vulnerabilities in the software. This could include activities before, during, and after the coding. **Processes:** Organisation should set up a process for defining the minimum baseline of secure coding – both for internal software development and for software

components from third parties, a process for monitoring emerging threats and advice on secure coding, a process for deciding which external tools and libraries can be used, and a process that defines activities done before the coding, during the coding, after the coding (review and maintenance), and for software modification.

Implementation:

Planning and before coding

a) Secure coding principles should be used both for new developments and in reuse scenarios.

b) These principles should be applied to development activities both within the organization and for products and services supplied by the organization to others.

c) Planning and prerequisites before coding should include:

1. organization-specific expectations and approved principles for secure coding to be used for both in-house and outsourced code developments;
2. common and historical coding practices and defects that lead to information security vulnerabilities;
3. configuring development tools, such as integrated development environments (IDE), to help enforce the creation of secure code;
4. following guidance issued by the providers of development tools and execution environments as applicable;
5. maintenance and use of updated development tools (e.g. compilers);
6. qualification of developers in writing secure code;
7. secure design and architecture, including threat modelling;
8. secure coding standards and where relevant mandating their use;
9. use of controlled environments for development.

During coding

a) Considerations during coding should include:

1. secure coding practices specific to the programming languages and techniques being used;
2. using secure programming techniques, such as pair programming, refactoring, peer review, security iterations and test-driven development;
3. using structured programming techniques;
4. documenting code and removing programming defects, which can allow information security vulnerabilities to be exploited;
5. prohibiting the use of insecure design techniques (e.g. the use of hard-coded passwords, unapproved code samples and unauthenticated web services).

Testing should be conducted during and after development

a) Before software is made operational, the following should be evaluated:

	1. attack surface and the principle of least privilege; 2. Conducting an analysis of the most common programming errors and documenting that these have been mitigated. **Review and maintenance** a) After code has been made operational: 1. updates should be securely packaged and deployed; 2. reported information security vulnerabilities should be handled 3. errors and suspected attacks should be logged and logs regularly reviewed to make adjustments to the code as necessary; 4. source code should be protected against unauthorized access and tampering (e.g. by using configuration management tools, which typically provide features such as access control and version control). b) If using external tools and libraries, the organization should consider: 1. ensuring that external libraries are managed (e.g. by maintaining an inventory of libraries used and their versions) and regularly updated with release cycles; 2. selection, authorization and reuse of well-vetted components, particularly authentication and cryptographic components; 3. the licence, security and history of external components; 4. ensuring that software is maintainable, tracked and originates from proven, reputable sources; 5. sufficiently long-term availability of development resources and artefacts. c) Where a software package needs to be modified the following points should be considered: 1. the risk of built-in controls and integrity processes being compromised; 2. whether to obtain the consent of the vendor; 3. the possibility of obtaining the required changes from the vendor as standard program updates; 4. the impact if the organization becomes responsible for the future maintenance of the software as a result of changes; 5. compatibility with other software in use

For more information please refer to ISO 27001:2022 Standard.