PERPETUUM
CAPITAL

ISO 27001 & Annex A

Version 2022

ENGLISH

4 Context of the organization

4.1 Understanding the organization and its context: The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.

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; and
b) the requirements of these interested parties relevant to information security**.**

4.3 Determining the scope of the information security management system: The organization shall determine the boundaries and applicability of the information security management system to establish its scope.
When determining this scope, the organization shall consider:

a) the external and internal issues referred to in 4.1;
b) the requirements referred to in 4.2; and
c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.
The scope shall be available as documented information.

4.4 Information security management system: The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this International Standard.

5 Leadership

5.1 Leadership and commitment: Top management shall demonstrate leadership and commitment with respect to the information security management system by:

a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization.
b) ensuring the integration of the information security management system requirements into the organization's processes;
c) ensuring that the resources needed for the information security management system are available;
d) communicating the importance of effective information security management and of conforming to the information security management system requirements;
e) ensuring that the information security management system achieves its intended outcome(s);
f) directing and supporting persons to contribute to the effectiveness of the information security management system;
g) promoting continual improvement; and
h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

5.2 Policy: Top management shall establish an information security policy that:

a) is appropriate to the purpose of the organization;

b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives;
c) includes a commitment to satisfy applicable requirements related to information security; and
d) includes a commitment to continual improvement of the information security management system.
The information security policy shall:
e) be available as documented information;
f) be communicated within the organization; and
g) be available to interested parties, as appropriate.

5.3 Organizational roles, responsibilities and authorities: Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated.
Top management shall assign the responsibility and authority for:

a) ensuring that the information security management system conforms to the requirements of this International Standard; and
b) reporting on the performance of the information security management system to top management.

6 Planning

6.1 Actions to address risks and opportunities:

6.1.1 General: When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:

a) ensure the information security management system can achieve its intended outcome(s);
b) prevent, or reduce, undesired effects; and
c) achieve continual improvement.
The organization shall plan:
d) actions to address these risks and opportunities; and
e) how to

1) integrate and implement the actions into its information security management system processes; and
2) evaluate the effectiveness of these actions.

6.1.2 Information security risk assessment: The organization shall define and apply an information security risk assessment process that:

a) establishes and maintains information security risk criteria that include:

1) the risk acceptance criteria; and
2) criteria for performing information security risk assessments;

b) ensures that repeated information security risk assessments produce consistent, valid and comparable results;
c) identifies the information security risks:

1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and
2) identify the risk owners;

d) analyses the information security risks:

1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize;
2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and
3) determine the levels of risk;

e) evaluates the information security risks:

1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and
2) prioritize the analyzed risks for risk treatment.

The organization shall retain documented information about the information security risk assessment process.

6.1.3 Information security risk treatment: The organization shall define and apply an information security risk treatment process to:

a) select appropriate information security risk treatment options, taking account of the risk assessment results;
b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen;
c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted;
d) produce a Statement of Applicability that contains the necessary controls (see 6.1.3 b) and c)) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A;
e) formulate an information security risk treatment plan; and
f) obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.
The organization shall retain documented information about the information security risk treatment process.

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 communicated; and
e) be updated as appropriate.

The organization shall retain documented information on the information security objectives.
When planning how to achieve its information security objectives, the organization shall determine:

f) what will be done;
g) what resources will be required;
h) who will be responsible;
i) when it will be completed; and
j) how the results will be evaluated.

7 Support

7.1 Resources: The organization shall determine and provide the resources needed for the establishment, implementation, maintenance, and continual improvement of the information security management system.

7.2 Competence: The organization shall:

a) determine the necessary competence of person(s) doing work under its control that affects its information security performance;
b) ensure that these persons are competent on the basis of appropriate education, training, or experience;
c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and
d) retain appropriate documented information as evidence of competence.

7.3 Awareness: Persons doing work under the organization's control shall be aware of:

a) the information security policy;
b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and
c) the implications of not conforming with the information security management system requirements.

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) who shall communicate; and
e) the processes by which communication shall be affected.

7.5 Documented information:
7.5.1 General: The organization's information security management system shall include:

a) documented information required by this International Standard; and
b) documented information determined by the organization as being necessary for the effectiveness of the information security management system.

1) the size of organization and its type of activities, processes, products, and services;
2) the complexity of processes and their interactions; and
3) the competence of persons.

7.5.2 Creating and updating: When creating and updating documented information the organization shall ensure appropriate:

a) identification and description (e.g. a title, date, author, or reference number);
b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and
c) review and approval for suitability and adequacy.

7.5.3 Control of documented information: Documented information required by the information security management system and by this International Standard shall be controlled to ensure:

a) it is available and suitable for use, where and when it is needed; and
b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).
For the control of documented information, the organization shall address the following activities, as applicable:
c) distribution, access, retrieval and use;
d) storage and preservation, including the preservation of legibility;
e) monitoring changes (e.g. version control); and
f) retention and disposition.

Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.

8 Operation

8.1 Operational planning and control: The organization shall plan, implement, and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1.
The organization shall also implement plans to achieve information security objectives determined in 6.2
The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.
The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.
The organization shall ensure that outsourced processes are determined and controlled.

8.2 Information security risk assessment: The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a).
The organization shall retain documented information of the results of the information security risk assessments.

8.3 Information security risk treatment: The organization shall implement the information security risk treatment plan.
The organization shall retain documented information of the results of the information security risk treatment.

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation: The organization shall evaluate the information security performance and the effectiveness of the information security management system.
The organization shall determine:

a) what needs to be monitored and measured, including information security processes and controls;
b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;
c) when the monitoring and measuring shall be performed;
d) who shall monitor and measure;
e) when the results from monitoring and measurement shall be analyzed and evaluated; and
f) who shall analyze and evaluate these results.
The organization shall retain appropriate documented information as evidence of the monitoring and measurement results.

9.2 Internal audit: The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system:

a) conforms to

1) the organization's own requirements for its information security management system; and
2) the requirements of this International Standard;

b) is effectively implemented and maintained.

The organization shall:
c) plan, establish, implement and maintain an audit program(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit program(s) shall take into consideration the importance of the processes concerned and the results of previous audits;
d) define the audit criteria and scope for each audit;
e) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;

f) ensure that the results of the audits are reported to relevant management; and
g) retain documented information as evidence of the audit program(s) and the audit results.

9.3 Management review: Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.
The management review shall include consideration of:

a) the status of actions from previous management reviews;
b) changes in external and internal issues that are relevant to the information security management system;
c) feedback on the information security performance, including trends in:

1) nonconformities and corrective actions;
2) monitoring and measurement results;
3) audit results; and
4) fulfilment of information security objectives;

d) feedback from interested parties;
e) results of risk assessment and status of risk treatment plan; and
f) opportunities for continual improvement.

The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.
The organization shall retain documented information as evidence of the results of management reviews.

10 Improvement

10.1 Nonconformity and corrective action: When a nonconformity occurs, the organization shall:

a) react to the nonconformity, and as applicable:

1) take action to control and correct it; and
2) deal with the consequences;

b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:

1) reviewing the nonconformity;
2) determining the causes of the nonconformity; and
3) determining if similar nonconformities exist, or could potentially occur;

c) implement any action needed;
d) review the effectiveness of any corrective action taken; and

e) make changes to the information security management system, if necessary.
Corrective actions shall be appropriate to the effects of the nonconformities encountered.
The organization shall retain documented information as evidence of:
f) the nature of the nonconformities and any subsequent actions taken, and
g) the results of any corrective action.

10.2 Continual improvement: The organization shall continually improve the suitability, adequacy, and effectiveness of the information security management system.

PERPETUUM
CAPITAL

Statement of Applicability (SOA) ISO 27001:2022

Annex A

A.5 Organizational controls

A.5.1 Policies for information security: Information security policy and topic-specific policies should be defined, approved by management, published, communicated to, and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.

A.5.2 Information security roles and responsibilities: Information security roles and responsibilities shall be defined and allocated according to the organization's needs.

A.5.3 Segregation of duties: Conflicting duties and areas of responsibility shall be segregated.

A.5.4 Management responsibilities: Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies, and procedures of the organization.

A.5.5 Contact with authorities: The organization shall establish and maintain contact with relevant authorities.

A.5.6 Contact with special interest groups: The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.

A.5.7 Threat intelligence: Information relating to information security threats shall be collected and analyzed to produce threat intelligence.

A.5.8 Information security in project management: Information security shall be integrated into project management.

A.5.9 Inventory of information and other associated assets: An inventory of information and other associated assets, including owners, shall be developed, and maintained.

A.5.10 Acceptable use of information and other associated assets: Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented, and implemented.

A.5.11 Return of assets: Personnel and other interested parties, as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract, or agreement.

A.5.12 Classification of information: Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability, and relevant interested party requirements.

A.5.13 Labelling of information: An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.

A.5.14 Information transfer: Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.

A.5.15 Access control: Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.

A.5.16 Identity management: The full life cycle of identities shall be managed.

A.5.17 Authentication information: Allocation and management of authentication information shall be controlled by a management process, including advising personnel of appropriate handling of authentication information.

A.5.18 Access rights: Access rights to information and other associated assets shall be provisioned, reviewed, modified, and removed in accordance with the organization's topic-specific policy on and rules for access control.

A.5.19 Information security in supplier relationships: Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.

A.5.20 Addressing information security within supplier agreements: Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.

A.5.21 Managing information security in the ICT supply chain: Processes and procedures shall be defined and implemented to manage information security risks associated with the ICT products and services supply chain.

A.5.22 Monitoring, review and change management of supplier services: The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.

A.5.23 Information security for use of cloud services: Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.

A.5.24 Information security incident management planning and preparation: The organization shall plan and prepare for managing information security incidents by defining, establishing, and communicating information security incident management processes, roles and responsibilities.

A.5.25 Assessment and decision on information security events: The organization shall assess information security events and decide if they are to be categorized as information security incidents.

A.5.26 Response to information security incidents: Information security incidents shall be responded to in accordance with the documented procedures.

A.5.27 Learning from information security incidents: Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.

A.5.28 Collection of evidence: The organization shall establish and implement procedures for the identification, collection, acquisition, and preservation of evidence related to information security events.

A.5.29 Information security during disruption: The organization shall plan how to maintain information security at an appropriate level during disruption.

A.5.30 ICT readiness for business continuity: ICT readiness shall be planned, implemented, maintained, and tested based on business continuity objectives and ICT continuity requirements.

A.5.31 Legal, statutory, regulatory and contractual requirements: Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date.

A.5.32 Intellectual property rights: The organization shall implement appropriate procedures to protect intellectual property rights.

A.5.33 Protection of records: Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.

A.5.34 Privacy and protection of PII: The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.

A.5.35 Independent review of information security: The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.

A.5.36 Compliance with policies, rules and standards for information security: Compliance with the organization's information security policy, topic-specific policies, rules and standards shall be regularly reviewed.

A.5.37 Documented operating procedures: Operating procedures for information processing facilities shall be documented and made available to personnel who need them.

A.6 People controls

A.6.1 Screening: Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

A.6.2 Terms and conditions of employment: The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.

A.6.3 Information security awareness, education and training: Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.

A.6.4 Disciplinary process: A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.

A.6.5 Responsibilities after termination or change of employment: Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.

A.6.6 Confidentiality or non-disclosure agreements: Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed, and signed by personnel and other relevant interested parties.

A.6.7 Remote working: Security measures shall be implemented when personnel are working remotely to protect information accessed, processed, or stored outside the organization's premises.

A.6.8 Information security event reporting: The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.

A.7 Physical controls

A.7.1 Physical security perimeters: Security perimeters shall be defined and used to protect areas that contain information and other associated assets.

A.7.2 Physical entry: Secure areas shall be protected by appropriate entry controls and access points.

A.7.3 Securing offices, rooms and facilities: Physical security for offices, rooms and facilities shall be designed and implemented.

A.7.4 Physical security monitoring: Premises shall be continuously monitored for unauthorized physical access.

A.7.5 Protecting against physical and environmental threats: Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.

A.7.6 Working in secure areas: Security measures for working in secure areas shall be designed and implemented.

A.7.7 Clear desk and clear screen: Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.

A.7.8 Equipment siting and protection: Equipment shall be sited securely and protected.

A.7.9 Security of assets off-premises: Off-site assets shall be protected.

A.7.10 Storage media: Storage media shall be managed through its life cycle of acquisition, use, transportation, and disposal in accordance with the organization's classification scheme and handling requirements.

A.7.11 Supporting utilities: Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.

A.7.12 Cabling security: Cables carrying power, data or supporting information services shall be protected from interception, interference, or damage.

A.7.13 Equipment maintenance: Equipment shall be maintained correctly to ensure availability, integrity, and confidentiality of information.

A.7.14 Secure disposal or re-use of equipment: Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

A.8 Technological controls

A.8.1 User endpoint devices: Information stored on, processed by or accessible via user endpoint devices shall be protected.

A.8.2 Privileged access rights: The allocation and use of privileged access rights shall be restricted and managed.

A.8.3 Information access restriction: Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.

A.8.4 Access to source code: Read and write access to source code, development tools and software libraries shall be appropriately managed.

A.8.5 Secure authentication: Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.

A.8.6 Capacity management: The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.

A.8.7 Protection against malware: Protection against malware shall be implemented and supported by appropriate user awareness.

A.8.8 Management of technical vulnerabilities: Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.

A.8.9 Configuration management: Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.

A.8.10 Information deletion: Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.

A.8.11 Data masking: Data masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific, and business requirements, taking applicable legislation into consideration.

A.8.12 Data leakage prevention: Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store, or transmit sensitive information.

A.8.13 Information backup: Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.

A.8.14 Redundancy of information processing facilities: Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.

A.8.15 Logging: Logs that record activities, exceptions, faults, and other relevant events shall be produced, stored, protected, and analyzed.

A.8.16 Monitoring activities: Networks, systems and applications shall be monitored for anomalous behavior and appropriate actions taken to evaluate potential information security incidents.

A.8.17 Clock synchronization: The clocks of information processing systems used by the organization shall be synchronized to approved time sources.

A.8.18 Use of privileged utility programs: The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.

A.8.19 Installation of software on operational systems: Procedures and measures shall be implemented to securely manage software installation on operational systems.

A.8.20 Networks security: Networks and network devices shall be secured, managed, and controlled to protect information in systems and applications.

A.8.21 Security of network services: Security mechanisms, service levels and service requirements of network services shall be identified, implemented, and monitored.

A.8.22 Segregation of networks: Groups of information services, users and information systems shall be segregated in the organization's networks.

A.8.23 Web filtering: Access to external websites shall be managed to reduce exposure to malicious content.

A.8.24 Use of cryptography: Rules for the effective use of cryptography, including cryptographic key management, shall be defined, and implemented.

A.8.25 Secure development life cycle: Rules for the secure development of software and systems shall be established and applied.

A.8.26 Application security requirements: Information security requirements shall be identified, specified, and approved when developing or acquiring applications.

A.8.27 Secure system architecture and engineering principles: Principles for engineering secure systems shall be established, documented, maintained, and applied to any information system development activities.

A.8.28 Secure coding: Secure coding principles shall be applied to software development.

A.8.29 Security testing in development and acceptance: Security testing processes shall be defined and implemented in the development life cycle.

A.8.30 Outsourced development: The organization shall direct, monitor and review the activities related to outsourced system development.

A.8.31 Separation of development, test and production environments: Development, testing and production environments shall be separated and secured.

A.8.32 Change management: Changes to information processing facilities and information systems shall be subject to change management procedures.

A.8.33 Test information: Test information shall be appropriately selected, protected, and managed.

A.8.34 Protection of information systems during audit testing: Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.