**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. NOTE Determining these issues refers to establishing the external and internal context of the organization considered in Clause 5.4.1 of ISO 31000:2018[5].

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.

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;

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, including the processes needed and their interactions, in accordance with the requirements of this document.

**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.

NOTE Reference to “business” in this document can be interpreted broadly to mean those activities that are core to the purposes of the organization’s existence.

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;

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;

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 within the organization. Top management shall assign the responsibility and authority for:
a) ensuring that the information security management system conforms to the requirements of this document;
b) reporting on the performance of the information security management system to top management.
NOTE Top management can also assign responsibilities and authorities for reporting performance of the information security management system within the organization.

**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;
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 analysed risks for risk treatment.
**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; NOTE 1 Organizations can design controls as required, or identify them from any source.
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; NOTE 2 Annex A contains a list of possible information security controls. Users of this document are directed to Annex A to ensure that no necessary information security controls are

overlooked. NOTE 3 The information security controls listed in Annex A are not exhaustive and additional information security controls can be included if needed.
d) produce a Statement of Applicability that contains: — the necessary controls (see 6.1.3 b) and c)); — justification for their inclusion; — whether the necessary controls are implemented or not; and — the justification for excluding any of the Annex A controls.
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. NOTE 4 The information security risk assessment and treatment process in this document aligns with the principles and generic guidelines provided in ISO 31000[5].
**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. The organization shall retain documented information on the information security objectives. When planning how to achieve its information security objectives, the organization shall determine:
h) what will be done;
i) what resources will be required;
j) who will be responsible;
k) when it will be completed; and
l) how the results will be evaluated.
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.
**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. NOTE Applicable actions can include, for example: the provision of training to, the mentoring of, or the reassignment of current employees; or the hiring or contracting of competent persons.
**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) how to communicate.

**7.5** Documented information

**7.5.1** General The organization's information security management system shall include:
a) documented information required by this document; and
b) documented information determined by the organization as being necessary for the effectiveness of the information security management system.
NOTE The extent of documented information for an information security management system can differ from one organization to another due to:
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 document 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) control of 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.
NOTE Access can imply a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information, etc.