International Standard

ISO 22340

Security and resilience — Protective security — Guidelines for an enterprise protective security architecture and framework

Sécurité et résilience — Sûreté préventive — Lignes directrices pour une architecture et un cadre de sûreté préventive de l'entreprise

First edition
2024-11

Reference number
ISO 22340:2024(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 292, *Security and resilience*.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

This document aims to meet a global need for organizations to formulate and integrate their protective security controls in a way that is based on risk management principles and strategically aligned with the interests of the organization. It details an enterprise architecture and integrated framework within which a diverse suite of security-related policy, processes and practices can be coordinated.

Clarity on what protective security is, what it means, how it can be implemented, and how its benefits can be measured, will be helpful to managers, regardless of the sector. This is particularly important for the many organizations that have expended substantial resources on various security measures that have not necessarily been coordinated or informed by the full range of security risk. In an increasingly complex security environment, this document aims to provide clarity in this regard and to provide a basis for better enterprise security outcomes as a result.

This document:

a) Provides guidance on how organizations and their managers can implement and manage coherent protective security arrangements.

b) Demonstrates the critically important idea that effective security management is based on an understanding of risk and the application of risk management principles, and that the form and implementation of security controls (that protect an organization's assets) are integral to the long-term success of the organization. Security is a business enabler, not an overhead cost to the organization.

c) Defines and details the elements of protective security, outlines an enterprise protective security governance model and defines the roles and responsibilities necessary in delivering protective security outcomes.

d) Demonstrates the critical importance of establishing and sustaining an organizational culture supporting positive security behaviours: where all personnel and interested parties have a sense of shared ownership of security outcomes; and where all are authorized and competent to act in the security interests of the organization and invested in the security of the organization.

e) Outlines the importance of continuous improvement in relation to an organization's protective security.

This document is applicable for any organization and will be particularly useful for those that have had difficulty implementing risk-based frameworks appropriate to their security context. Organizations with such difficulties can be guided by this document in identifying and procuring appropriately competent services to assist.

The guidelines contained in this document do not provide detailed procedures at the technical or operational level. Where standards are not available at this level, organizations should formulate and implement procedures based on the high-level guidance contained in this document and according to best practices at international and national levels.

Security and resilience — Protective security — Guidelines for an enterprise protective security architecture and framework

1 Scope

This document provides guidance on the enterprise protective security architecture and the framework of protective security policies, processes and types of controls necessary to mitigate and manage security risks across the protective security domains, including:

a) security governance;

b) personnel security;

c) information security;

d) cybersecurity;

e) physical security.

This document is applicable for any organization.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 22300, *Security and resilience — Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22300 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
asset owner
person within the organization who is responsible for a given asset

3.2
business impact
impact on an organization's or sector's ability to operate resulting from the compromise of confidentiality, integrity or availability of assets

3.3
culture
shared values and attitudes that are applied within an organization by its personnel and interested parties

Note 1 to entry: This recognizes that an organization has a culture that, to varying degrees, supports and accepts security as part of business as usual; and that fostering this element of the organization's culture should be the aim of top management in delivering protective security outcomes.

3.4
cybersecurity
protection of the confidentiality, integrity, and availability of digital systems (hardware, software and associated infrastructure) from unauthorized digital access, harm or misuse, or attack scenarios that involve deliberate exploitation of computer systems, digitally-dependent enterprise networks and control systems

Note 1 to entry: This relates to a range of technical *domains* (3.5), including but not necessarily limited to *information and communications technology (ICT)* (3.9) and operational technology (OT).

3.5
domain
defined sphere of *protective security* (3.17) activity or knowledge

3.6
enterprise protective security architecture
documented structure comprising governance arrangements and the security framework elements by which protective security functions are performed and strategically aligned with the aims of the organization

3.7
framework
structure of policies, processes and specifications designed to support the accomplishment of an objective

Note 1 to entry: In this connection, a protective security framework consists of and aligns all elements of protective security policy and processes, including security *governance* (3.8), *personnel security* (3.15), *information security* (3.12), *cybersecurity* (3.4) and *physical security* (3.16).

3.8
governance
system of directing and controlling

Note 1 to entry: The processes by which organizations are directed, controlled and held to account, encompassing authority, accountability, stewardship, leadership, direction and control exercised in the organization.

3.9
information and communications technology
ICT
technology for gathering, storing, retrieving, processing, analysing and transmitting information

[SOURCE: ISO/IEC 30071-1:2019, 3.2.5]

3.10
information asset
knowledge or data that have value for the individual or organization (including intellectual property), which are defined and managed so it can be understood, shared, protected and used

3.11
information life cycle
process whereby information is managed over time, from the point of creation, receipt, distribution, use, maintenance and final disposal (disposition, destruction or archiving) according to the business impact of reduction or loss of the confidentiality, integrity or availability of information

3.12
information security
protection and preservation of the confidentiality, integrity and availability of all *information assets* (3.10), including information in transit (e.g. transactional security), digital security and *cybersecurity* (3.4)

Note 1 to entry: Information security relates to the security of information in all its forms (including hard copy and verbal communications), digital systems, *information and communications technology (ICT)* (3.10) and *operational technology (OT)*.

Note 2 to entry: Additional properties, such as authenticity, accountability, non-repudiation and reliability, can be included.

[SOURCE: ISO/IEC 27000:2018, 3.28, modified — definition has been extended and note 1 to entry has been added.]

3.13
measure
action or means to eliminate hazards or reduce risks

[SOURCE: ISO/IEC Guide 51:2014, 3.13, modified — example has been removed]

3.14
need-to-know
need to access specific information based on a business or operational requirement according to an active process of determining the security level of information and who has the right to access the information

3.15
personnel security
process of gaining and maintaining assurance of a person's eligibility and suitability (honesty, trustworthiness, maturity, resilience, loyalty and security competence) to access organizational assets

3.16
physical security
combination of physical *security controls* (3.19) to reduce the risk of unauthorized access, to safeguard assets and to protect from a potential security incident

3.17
protective security
processes and activities that protect assets from malicious acts, the impact of unintentional incidents and other events that can cause harm

Note 1 to entry: Protective security includes the following domains: security *governance* (3.8), *personnel security* (3.15), *information security* (3.12), *cybersecurity* (3.4) and *physical security* (3.16).

3.18
responsible security executive
RSE
person assigned within the organization's top management as the single point of responsibility for managing the organization's *security risk* (3.21)

Note 1 to entry: Having responsibility for managing the organization's security risk, the RSE is accountable to top management for the performance of that task. Top management is in turn accountable for the overall performance of the organization in general.

Note 2 to entry: The RSE is responsible for ensuring that the organization's security function is effectively managed and provides assurance to top management that security risks are being actively managed.

Note 3 to entry: Proper *governance* (3.8) requires that the RSE has the authority, resources and competence necessary to exercise this responsibility; and is part of, or has effective access to, top management.

3.19
security control
policy, process, or tangible or intangible risk reduction application which, on the basis of assessment, is implemented to treat risk by reducing or maintaining the likelihood of a security-related risk being realised, within specific levels or ranges

Note 1 to entry: This includes but is not limited to digital and physical access controls, alarms, active and passive surveillance, vetting and other personnel assessment tools.

Note 2 to entry: A security treatment is the actual application or implementation of one or more security controls to achieve an acceptable level of risk.

3.20
security in depth
defence in depth
protection in depth
use of multiple protective *security controls* (3.19) in layers across the enterprise to protect assets

Note 1 to entry: This recognizes that the strength of any system is no greater than its weakest link and ensures that if one control element fails, other defensive *measures* (3.13) are in place to continue providing protection.

3.21
security risk
potential that malicious actors (or any unintentional action or event) could harm or result in compromise, loss or unavailability of an organization's assets or reduce the effectiveness of *security controls* (3.19)

Note 1 to entry: See *security threat* (3.22).

Note 2 to entry: This definition draws on the definition of risk according to ISO 31000:2018, 3.1, in the context of security risk, where uncertainty in relation to the intent and capability of malicious actors and vulnerability to their actions can impact objectives.

3.22
security threat
threat that arises when the intentions and capabilities of malicious actors are committed to action and intersect with the vulnerabilities of protective *security controls* (3.19) or the intrinsic systems of an organization

Note 1 to entry: A vulnerability can be inherent in an asset or process or be caused by any event or circumstance, including a natural event or accident.

Note 2 to entry: Threat is sometimes considered as analogous to hazard (potential source of harm), although in the security context, hazard typically refers to materials or tools pre-existing in the operating environment that can be used by a malicious actor, such as explosives, malware, etc.

3.23
security vetting
processes designed to verify the identity of personnel and to provide assurance that they are eligible and suitable to access organizational assets

4 Enterprise protective security architecture

4.1 General

Protective security is optimized when it is aligned with protective security principles and led by the organization's top management. In that respect, the organization should implement governance arrangements that provide enterprise-level appreciation of security and deliver a framework of protective security policies, processes and specifications that are strategically aligned within the business.

4.2 Integration

Governance arrangements inform a security management programme which in turn should be incorporated within business operations in order to achieve the organization’s security objectives.

The enterprise protective security architecture outlined in this document consists of the principles, governance arrangements and structural elements within which the framework of protective security policies, processes and specifications are implemented and managed.

Organizing security management along these lines requires support throughout the entire organization and strong leadership from top management and asset owners in particular. Also, since effective security risk management is key to security outcomes, the organization should undertake risk processes consistent with ISO 31000:2018, Clause 6 and ensure that all elements of security governance operate consistently with ISO 31000 in general.

Organizations should identify specific technical standards according to the need or, if these are not available, formulate and implement procedures based on the guidance contained in this document and according to best international and national practice.

Controls not directly related to security, but which can mitigate or accentuate security risk (emergency management and response, business continuity, crisis management, safety and privacy for example), should also be aligned within this enterprise protective security architecture.

4.3 Elements of the architecture

The organization should implement an enterprise protective security architecture consisting of the elements specified in Table 1.

Table 1 — Elements of the enterprise protective security architecture

Level		**Description**
1	Governance level: Protective security principles	The principles that drive strategy, objectives, resourcing and review of protective security at the organizational leadership and governance level.
2	Management level: Protective security domains	The domains of security practice that achieve these guiding principles in terms of the security of the organization’s assets.
3	Implementation, operations and review level: Security risk management	The management of security risks enabling delivery of the objectives of the organization. Controls are implemented to mitigate/modify/treat security risk in relation to each of the security domains: security governance, personnel security, information security, cybersecurity, and physical security. A converged approach ensures that application of controls is complementary to the required security outcomes. Processes for measuring performance and for continuous improvement are included at this level.
	NOTE Monitoring performance is expanded upon in 6.2.2.7 and 6.2.2.8 and Clause 11.	

Elements of the enterprise protective security architecture can be expanded to align with the more detailed framework of organizational arrangements for security as outlined in Figure 1. Relevant technical standards can also assist in applying risk treatments. If these are not available, the organization should formulate and implement procedures based on this document.

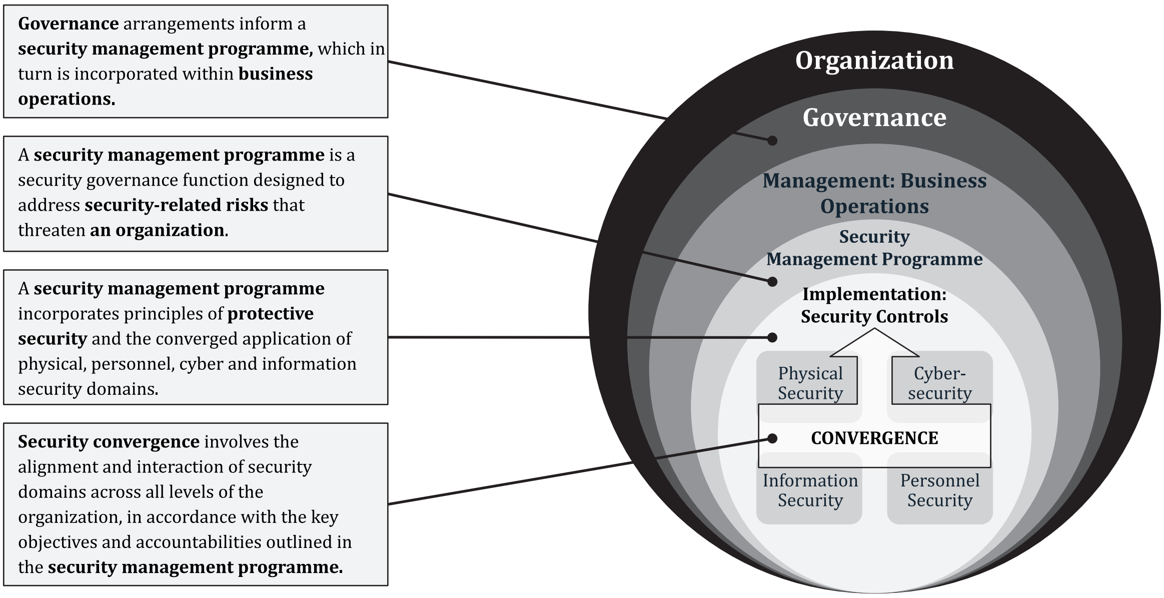

Governance arrangements inform a **security management programme,** which in turn is incorporated within **business operations.**
A **security management programme** is a security governance function designed to address **security-related risks** that threaten **an organization.**
A **security management programme** incorporates principles of **protective security** and the converged application of physical, personnel, cyber and information security domains.
Security convergence involves the alignment and interaction of security domains across all levels of the organization, in accordance with the key objectives and accountabilities outlined in the **security management programme.**
Organization
Governance
Management: Business Operations
Security Management Programme
Implementation: Security Controls
Physical Security
Cyber-security
CONVERGENCE
Information Security
Personnel Security

Figure 1 — Expanded architecture and framework view

5 Protective security principles and domains

5.1 Protective security principles

The organization should be guided by the following protective security principles when formulating and executing security strategies, policies, procedures, processes and operations:

a) Security is everyone's responsibility: a positive culture, where everyone has an active role to play, is critical to security.

b) Security enables business: security supports the organization's mission and the delivery of its products and services.

c) Security management is based on risk management principles and methodology: security controls are applied proportionately to protect the organization's assets according to the organization's overall assessed risk.

NOTE 1 An asset is anything that is of value to the organization, such as human, physical, information, intangible, environmental and infrastructure resources. Human assets include employees, contractors or other interested parties. Assets do not necessarily have to belong to the organization.

d) Top management is accountable for the organization's security: top management owns the risks of their organization, invests in and sponsors the organization's security, delegates responsibility according to competence and resources; and holds accountable those to whom responsibility has been delegated.

e) Security is integrated into all levels of the organization's activity: security risk is managed through protective security controls that are coordinated across the organization.

f) Security is delivered within a life cycle of continual improvement: a cycle of action, evaluation and learning is implemented to identify improvement opportunities, to assess and reassess the effectiveness of controls and to define options for corrective actions.

The organization should integrate security principles, thinking and practice into all levels of decision making and activity to enable effective management of security risk. Responsibility for the day-to-day management of security should be delegated by the RSE according to competence and resources.

NOTE 2 Although not necessarily personally involved, top management remains accountable for the overall performance of the organization, including its security.

5.2 Protective security domains

The above protective security principles are delivered by managing security risks to the organization through the application of controls in the following domains:

a) security governance;

b) personnel security;

c) information security;

d) cybersecurity;

e) physical security.

As reflected in Figures 1 and 2, these domains are not mutually exclusive. They are connected and impact one another. In applying risk management, the organization should ensure that security risk is assessed and managed within a framework of coordinated planning and implementation of security controls across all of these domains. In addition to implementing the processes to deliver this coordinated approach, the organization should develop the supporting policy, procedures and processes needed to implement, operate, and test each control.

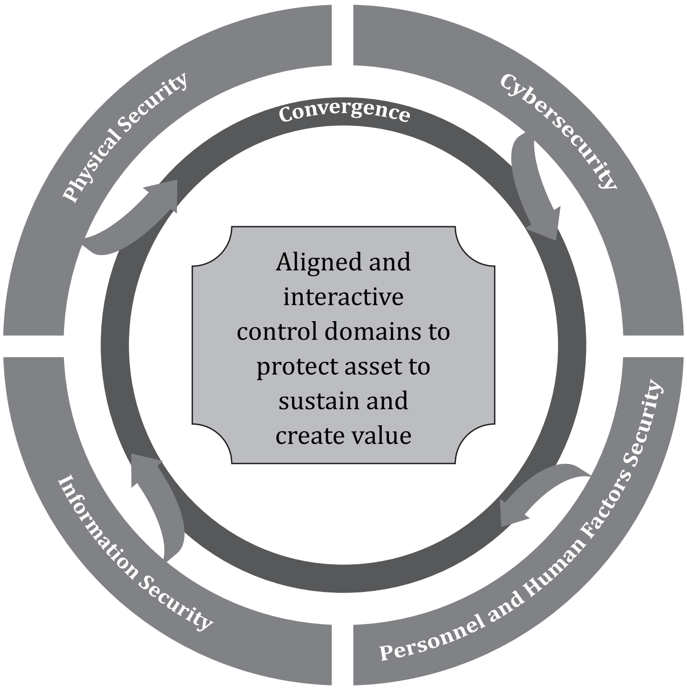

Physical Security
Cybersecurity
Convergence
Aligned and interactive control domains to protect asset to sustain and create value
Information Security
Personnel and Human Factors Security

Figure 2 — Convergence of security domains to protect assets

6 Security governance domain

6.1 Objective

Effective governance of security ensures that the enterprise protective security architecture delivers security outcomes that protect the organization’s assets, enabling the organization to achieve its objectives.

In the security governance domain, the organization should aim to:

— manage security risks and support a positive security approach in the organization’s culture, ensuring clear accountabilities and lines of responsibility, effective planning, proper integration and coordination, assurance, review and improvement processes and proportionate reporting.

The organization's top management (the board, chief executive officer, head of agency, etc.) should delegate responsibility for the organization's security to the responsible security executive (RSE). While delegating this responsibility, top management nonetheless retains accountability for the outcome of the delegated work. This means that top management is accountable for the outcomes of the application of security management, and that those given responsibilities for implementing controls will be held accountable for the outcomes of those controls.

The RSE should be a member of, or have authoritative access to, top management. Also, the organization should ensure effective reporting and communication of security risk occurs between top management and the RSE.

The RSE has final authority in defining the organization's security footing. Also, in coordination with top management and asset owners, the RSE is primarily responsible for ensuring that the organization's security risk is managed and its security outcomes are delivered.

The RSE should have adequate operational resources to lead, promote and manage the security of the organization. Depending on the size of the organization, other executives or managers should be assigned to security functions under the RSE to manage organizational security. Security managers may hold other managerial roles but should be professionally competent in security and have the capacity to fulfil their roles effectively.

In small organizations, the security function may be conducted by proportionately smaller management structures. However, an RSE should still be appointed and identified.

6.2 Security controls

6.2.1 The responsible security executive

In implementing the organization's framework of protective security policies, the roles and responsibilities of the RSE include, but are not necessarily limited to:

a) understanding the organization's business and being able to engage effectively with top management and oversight bodies, as applicable, to enable effective management of security risk;

b) using security expertise to guide asset owners through the security risk management decision-making process for their respective assets;

c) understanding, managing and reporting on the implications that risk management decisions may have on other organizations and sharing this information where appropriate;

d) promoting an understanding throughout the organization that security is everyone's business, and that all personnel, contractors and any other people working on behalf of the organization, share responsibility for maintaining a secure workplace;

e) being competent and knowledgeable regarding the ethical considerations of security and how risk management fits within the whole-of-organization context;

f) defining and implementing an organizational culture that accepts and supports security processes;

g) ensuring personnel contractors and any other people working on behalf of the organization, are provided with sufficient information and training to support their shared responsibility;

h) ensuring that security risk management is integrated with the organization's security principles at the enterprise level;

i) facilitating agreement on the amount and type of security risk that can potentially be taken by the organization;

j) managing and reporting on the security risks of their organization, including briefing the CEO, board and/or audit and risk committee (or equivalent) on the security of the organization and proposing, leading and managing appropriate security risk management action.

6.2.2 Security management structure

6.2.2.1 General

The organization should implement an appropriately resourced security management structure to be managed by the RSE. The work that this group does should be based upon risk management as detailed in 6.2.2.2 and 6.2.2.3.

6.2.2.2 Managing security risk

The RSE should ensure that a risk management process is applied consistently across the protective security domains, and in a way that is appropriate to the security risk context of the organization. Risks in relation to these domains should be included in security risk assessments of specific parts of the organization's business (e.g. major projects, sensitive operations, transactions, transportation, organizational resilience). Security plans and corresponding controls should be implemented as part of this process.

The organization should be proactive in managing risk by gathering, analysing and responding to information on threats. Threat actors can originate internationally, nationally and in the community in which the organization is located and from which it draws its personnel. Organizations have intrinsic intelligence capabilities: their people and networks in their interested party communities that can be utilized for gaining an appreciation of emerging threats and in managing the associated risks. In addition, the organization's understanding of threat should be informed by a range of other inputs, such as security incident reporting provided by related organizations and information flows from government agencies and law enforcement authorities.

This should also be informed by the assessed vulnerability of assets to attack and their value to the business. The organization should implement protective measures commensurate with the value of assets in terms of the business impact of compromise or loss.

Management of enterprise security on the basis of risk requires a programme of work in which security risk is consistently assessed on an ongoing basis, giving rise to a single and coordinated picture of the security-related risks to the organization. Accordingly, the organization should be able to be informed of relevant security risks in its decision-making process. Guidelines on how this can be achieved are outlined in 6.2.2.3.

6.2.2.3 Security programme

6.2.2.3.1 General

In developing the programme by which security risk will be managed, the organization should use the security risk management process model derived from ISO 31000, including the range of elements that relate to the organization's internal and external environment and its management requirements (see Figures 3 to 8 and the associated lists of attributes).

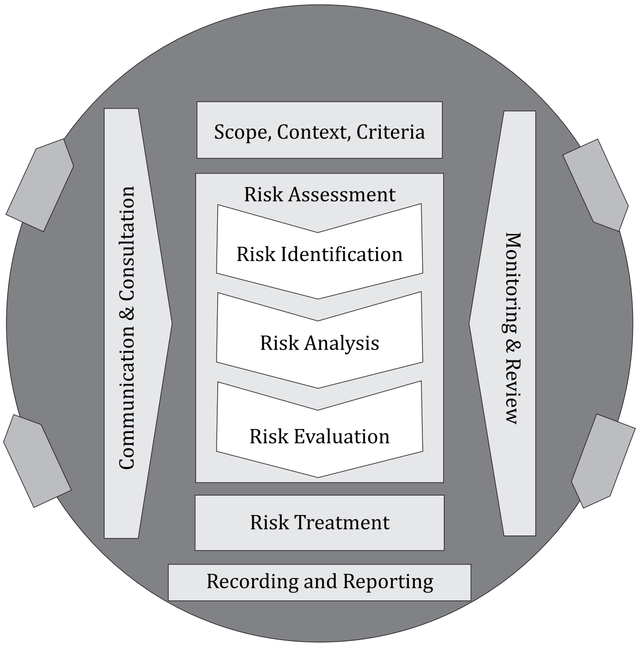


Figure 3 — ISO 31000 risk management process

6.2.2.3.2 Scope

The scope of the organization’s security programme and the risk management processes implemented to deliver it should be informed by following attributes:

a) Requirements to achieve organizational objectives

Known and potential sources of security risk and their likely impact on the achievement of organizational objectives.

b) Governance, policy and processes

Existing arrangements for accountability and responsibility in relation to the organization’s security and the security-related policies and implementing processes, and their respective impact in relation to security risk and the security programme itself.

6.2.2.3.3 Context

The organization should maintain a detailed and up-to-date understanding of its security context, including:

a) Organizational operating environment

Examine the security in the operating environment, including local, national and geopolitical considerations.

b) Organizational management

Understand the effectiveness of the alignment between organizational management practices and procedures with the management and delivery of security objectives.

c) The organization’s assets

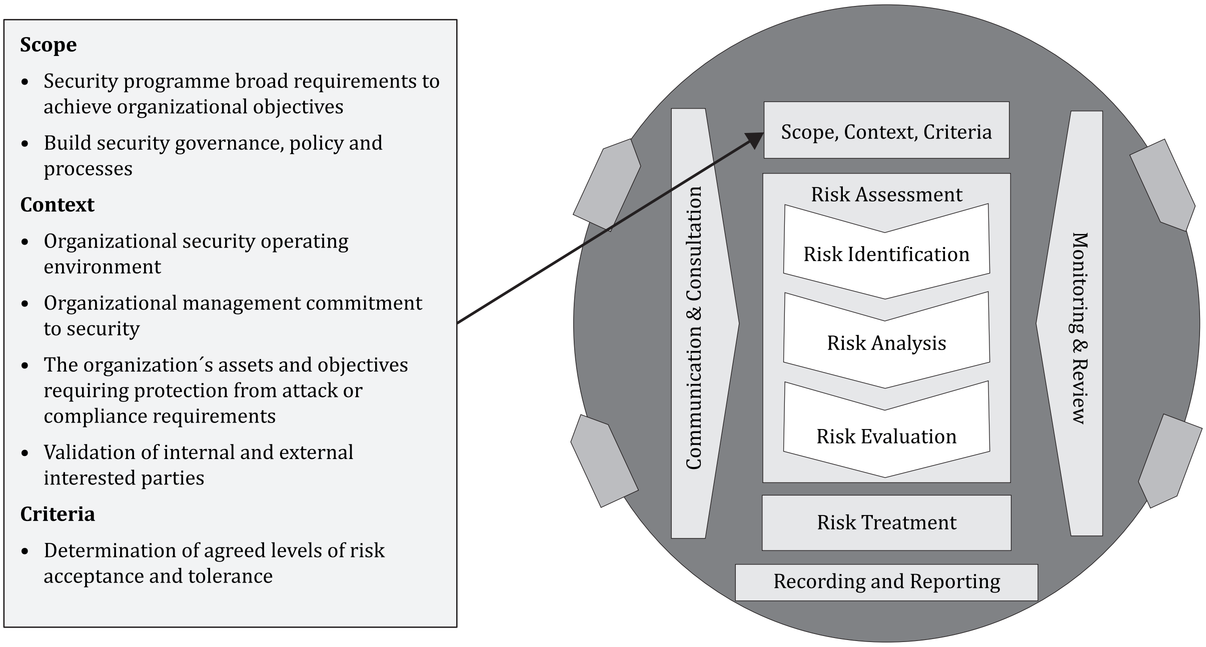
Identify the assets critical to the organization’s objectives that can be vulnerable to a security-related threat.

d) Validation of internal and external interested parties

Confirm the parties that are required to participate, provide resources in support of, or who can be impacted by, the organization's response to security risk.

6.2.2.3.4 Criteria

In delivering effective risk management, the organization should develop a clear understanding of the criteria by which it will understand, plan for and respond to risk. This requires the organization to determine the amount and type of security-related risks to its objectives that it may or may not take. Conversely, an outcome of risk management is to identify the responses and controls that will be required to treat security-related risks that are assessed as having impacts on objectives within the organization's risk tolerance. These risks can be accepted by the organization.



Scope

- Security programme broad requirements to achieve organizational objectives
- Build security governance, policy and processes

Context

- Organizational security operating environment
- Organizational management commitment to security
- The organization´s assets and objectives requiring protection from attack or compliance requirements
- Validation of internal and external interested parties

Criteria

- Determination of agreed levels of risk acceptance and tolerance

Figure 4 — Security risk management scope, context and criteria

6.2.2.3.5 Communication and consultation

Communication and consultation with stakeholders are critically important in understanding, analysing and managing security-related risk. Attributes of effective communication and consultation include:

a) Communications strategy

In consideration of communications and consultation, there should be a planned approach to engage with all those validated as internal and external interested parties.

b) Client and interested party requirements

As a result of the communication and consultation process, consideration of the security requirements of those parties should be included in the assessment and management processes.

c) Privacy

The privacy of all participants should be respected and where personal information is relevant to the assessments, appropriate protections should be implemented.

d) Confidentiality

Information required for, or gathered during, the assessment phase, should be allocated an appropriate level of confidentiality to reflect the participants and their contribution and to ensure actions recommended by the assessment cannot be accessed by those who are a source of security risk.

e) Consent

Consent of participants should be confirmed to ensure that they are aware of the individual and collective consequences arising from the assessment.

f) Sources of validation

Sources of validation for an assessment include, but are not necessarily limited to, existing policies and processes, open-source information and information available from reputable authorities. Checking against such sources serves to validate the underlying assumptions of the assessment.

g) Process guidance

There should be clear, documented guidance on how an assessment will be undertaken. Where appropriate, this guidance should be provided to interested parties.

h) Roles

Those performing the roles of communicators, analysts, assurers, reviewers and reporters should understand the appropriate security domains and their disciplines. Also, the participants in this assessment should be conversant with their respective roles and competent to perform them.

i) Information access and use

Arrangements should be implemented regarding access to and use of information relating to the risk assessment. Need-to-know and need-to-share principles should be determined according to the sensitivity of the risk assessment and the information that is generated in its development.

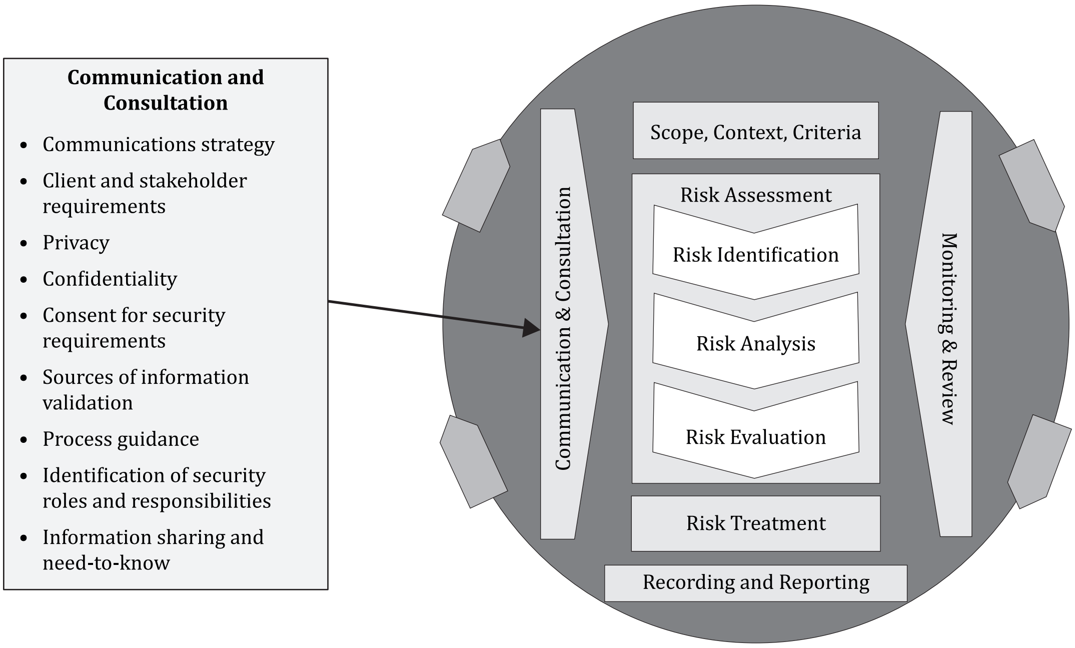

Communication and Consultation
- Communications strategy
- Client and stakeholder requirements
- Privacy
- Confidentiality
- Consent for security requirements
- Sources of information validation
- Process guidance
- Identification of security roles and responsibilities
- Information sharing and need-to-know
Communication & Consultation
Scope, Context, Criteria
Risk Assessment
Risk Identification
Risk Analysis
Risk Evaluation
Risk Treatment
Recording and Reporting
Monitoring & Review

Figure 5 — Security risk management process communication and consultation

6.2.2.3.6 Recording and reporting

In developing its security records policy and management system, the organization should align as far as possible with its general records management. A specific security records policy should take into account special handling procedures for individual items of information, or information that has been aggregated as a consequence of the risk assessment process.

a) Security records policy

The organization's security records policy should reflect the level of security required for the protection of the information to be used in the assessment, the validity and reliability standards for information to be included in records and guidance on the access control/need-to-know of the material in such records.

b) Records management system

The records management system associated with a risk assessment or with security management generally, should ensure the application of appropriate security controls regarding the integrity, confidentiality and availability of the information used within the risk assessment or management process, or that it is developed as a consequence of that process.

c) Access to documentation

The organization should apply security measures to ensure the integrity, confidentiality and availability, and allowing access to relevant information for those who have a need-to-know.

d) Reporting channels

Suitably controlled reporting channels should enable timely reporting of information to appropriate internal and external parties with a need-to-know. Whether channels are provided digitally, verbally or in hard copy, specific security controls should be in place to maintain integrity, confidentiality and availability.

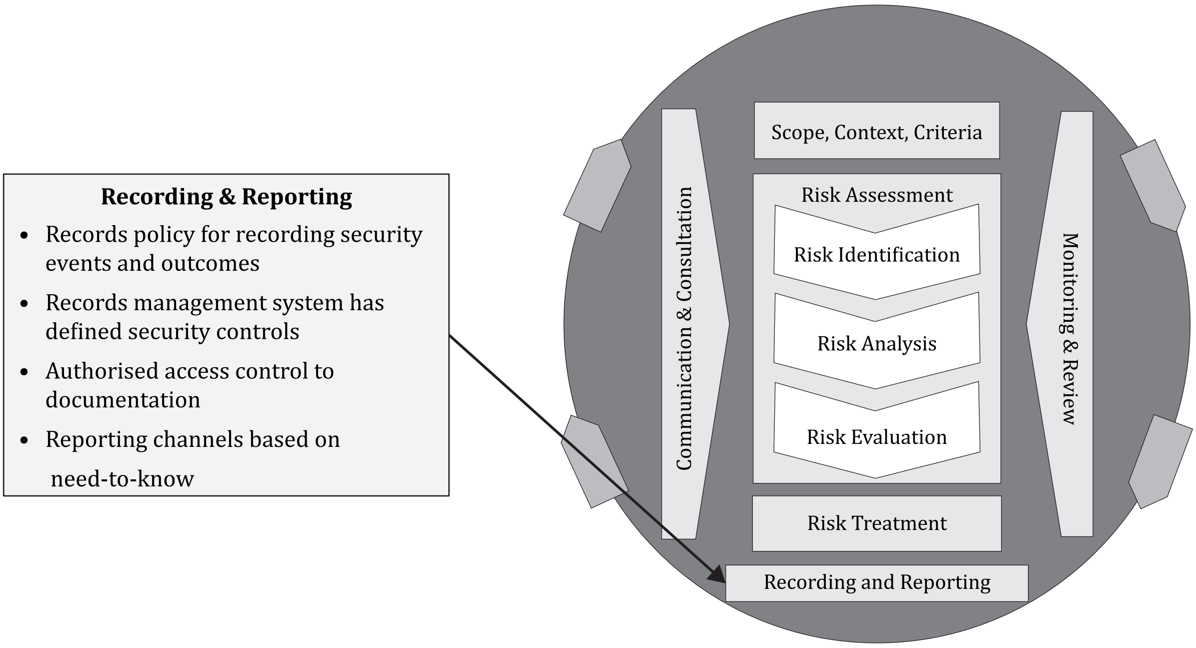

Recording & Reporting
Records policy for recording security events and outcomes
Records management system has defined security controls
Authorised access control to documentation
Reporting channels based on need-to-know
Scope, Context, Criteria
Risk Assessment
Risk Identification
Risk Analysis
Risk Evaluation
Risk Treatment
Recording and Reporting
Communication & Consultation
Monitoring & Review

Figure 6 — Security risk management process reporting and recording

6.2.2.3.7 Monitoring and review

A security risk assessment can generate information that is highly sensitive to the organization, for example, its personnel security risk assessment. This can represent considerable vulnerability in relation to a range of security threat. Consequently, in monitoring and reviewing the risk assessment and subsequent management process, the organization should give consideration to the roles of all persons involved and the level of trust and access required to achieve the desired outcomes.

a) Accountability

In order to hold individuals accountable, the levels and nature of accountability should reflect the designated roles of those involved in the assessment, which can include: the effectiveness of the application of security controls; the sustainment of information integrity, confidentiality and availability; and the quality and nature of the output of the assessment.

b) Responsibility

The individuals involved in an assessment should understand what they are responsible for delivering in the process and be held accountable for any shortcomings.

c) Consistency

In defining the attributes of a risk assessment process, the organization should ensure that all parties involved have a common understanding and complementary approaches to the assessment work. Also, security controls should be applied consistently across all aspects of the assessment.

d) Probity and integrity

Those selected to develop a risk assessment should be able to demonstrate the highest level of moral principles and adherence to those principles as they relate to security, thus ensuring the probity and integrity of the risk assessment system.

e) Audit

An official inspection and review should be undertaken of a risk assessment process to ensure the security, effectiveness and efficiency of the process.

f) Assurance

The external auditor of the accountable person should provide assurance that the security of an assessment or assessments has not been compromised and that the material developed in the assessment is fit for purpose.

g) Policy and process review

The organization should audit and review its risk assessment process periodically and amend it as necessary according to changes in the security and management context.

6.2.2.4 Risk assessment and treatment

6.2.2.4.1 General

The organization should apply the following approach and processes to assessing risk and identifying controls and subsequent application of treatments, or specific options for addressing risk as described in ISO 31000:2018. These are illustrated in Figure 7 and include the elements explained in 6.2.2.4.2 to 6.2.2.4.4.

6.2.2.4.2 Risk analysis

In analysing risks, the organization should include:

a) Impact analysis of harm to, or compromise of, sensitive or valuable assets, including the following attributes and others according to the context of the analysis:

- Economic or financial (e.g. impact on operating budget);
- Legal (e.g. non-compliance with legislation, commercial confidentiality, and legal privilege);

- Personal (e.g. impact on the personal safety, dignity, finances, liberty, or identity of a person or persons);
- Service delivery (e.g. capacity to operate, deliver services or programmes, reputation, confidence, and utilization of services);

b) Determination of a level of certainty in relation to the credibility and timeliness of the available information;

c) Appreciation of the volatility, or rate of change in these variables; and

d) The likelihood and the potential for risks to occur.

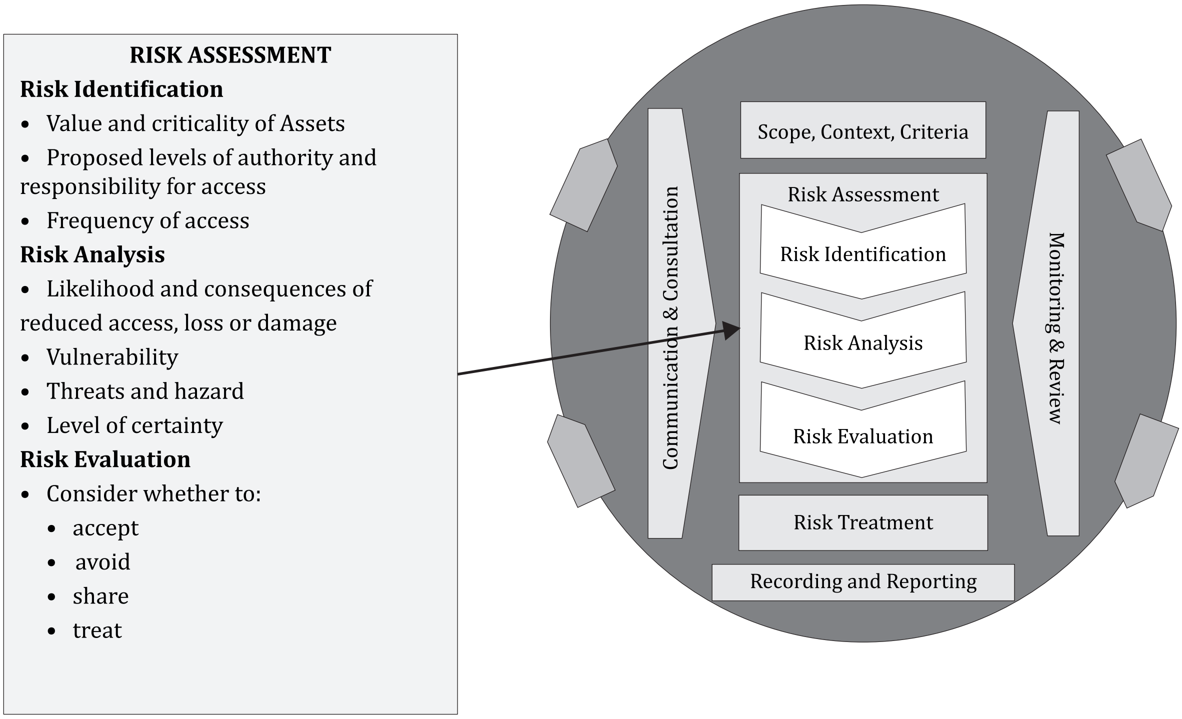
6.2.2.4.3 Risk evaluation

In identifying and evaluating risks, the organization should consider the value and criticality of sensitive or valuable assets and the vulnerability of assets and sources of threat.

The purpose of risk evaluation is to provide the analytical basis for decisions intended to modify risk. Risk evaluation in the security context (the actions of malicious actors) should at least include evidence-based evaluations of the potential for loss or damage to assets; for loss, shortage or other impact on the organization’s products or outputs; reputation impacts; impacts on clients, customers and other key stakeholders; and loss of competitiveness.

Such evaluation involves comparing the results of the risk analysis with the established risk criteria to determine where additional action is required on the basis of the agreed level of risk acceptance. In line with this, the analysis should consider as a minimum the necessity to:

- do nothing further;
- consider risk treatment options;
- undertake further analysis to better understand the risk;
- maintain existing controls;
- reconsider objectives.



RISK ASSESSMENT

Risk Identification

- Value and criticality of Assets
- Proposed levels of authority and responsibility for access
- Frequency of access

Risk Analysis

- Likelihood and consequences of reduced access, loss or damage
- Vulnerability
- Threats and hazard
- Level of certainty

Risk Evaluation

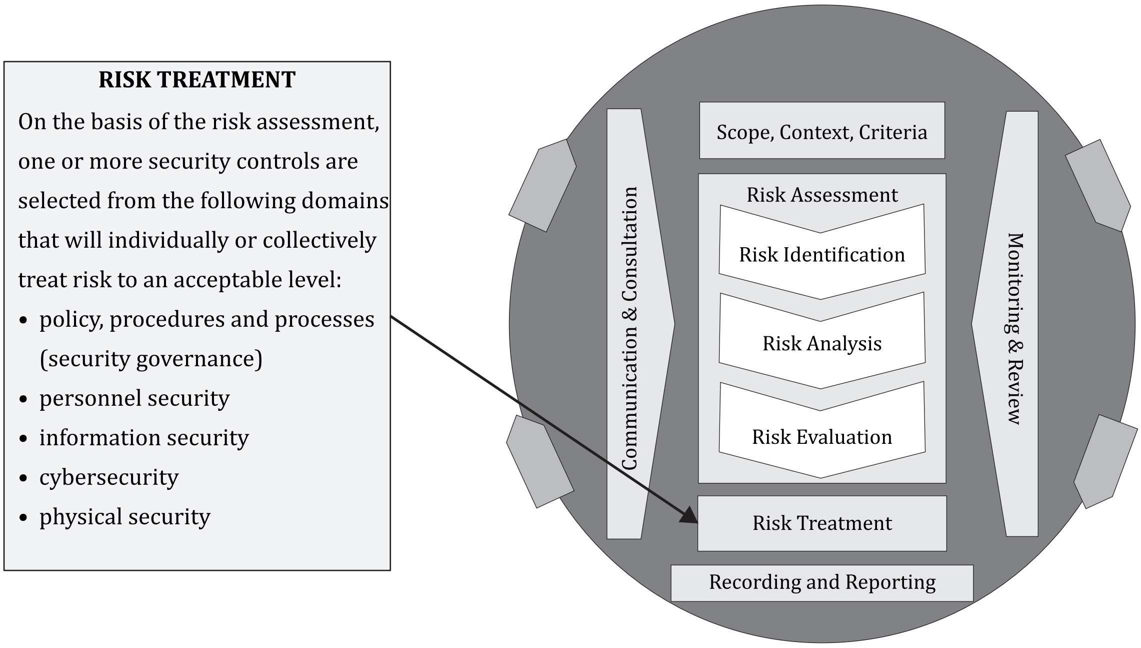
- Consider whether to:
  - accept
  - avoid
  - share
  - treat

Figure 7 — Security risk management identification, analysis and evaluation

6.2.2.4.4 Risk treatment

The organization should select controls from the security governance and the personnel, information, cyber and physical security domains to treat identified security related risk. Importantly, the organization should also regularly review the effectiveness of controls in treating risk and implement improvements where necessary.

Guidance for risk assessment methods is available in IEC 31010.



RISK TREATMENT

On the basis of the risk assessment, one or more security controls are selected from the following domains that will individually or collectively treat risk to an acceptable level:

- policy, procedures and processes (security governance)
- personnel security
- information security
- cybersecurity
- physical security

Figure 8 — Security risk management treatment process

6.2.2.5 Security planning

The organization should develop and implement a security plan, which should include:

a) how security risk management interacts with and enables the organization’s strategic objectives and priorities;

b) the security risks and vulnerabilities of the organization and their impact on the protection of the organization’s assets;

c) the amount and type of risk the organization is prepared to accept;

d) detail of the organization’s strategies, including controls and application of treatments, to manage security risks;

e) details of related change management planning regarding the transition to a more mature organizational culture that accepts and supports security processes;

f) coordinated response planning in relation to variations in the threat environment and subsequent security risk;

g) the status of the organization’s security plan and how this is reported.

Security plans should be reviewed regularly. Additional reviews can be necessary arising from changes to the organization’s context, including but not necessarily limited to changes in objectives, strategy, structure, technology, assets and operating environment.

Security plans should be reviewed for currency and effectiveness regularly, as part of a post incident review, and when significant changes to the organizational structure occur.

Where security controls are mandated by law, it is expected that the security plan includes provisions for their implementation. Mandated controls will not necessarily treat security risk to acceptable levels and additional controls can be necessary. The organization should proactively seek to understand and diligently manage its security risk.

6.2.2.6 External engagement

The security interests and impacts of external interested parties are relevant to the organization’s security risk and risk management. The organization should proactively engage with external interested parties and organizations. These interdependences should be reflected in security planning and utilized to optimize interoperability, coordination of planning and response and information exchange on security risk.

6.2.2.7 Security performance

The organization should monitor security capability and progress against the strategic objectives and goals identified in the organization’s security plan and strengthen the organization’s security maturity and culture of security. The organization should focus on how effectively it:

a) minimises risk to its assets;

b) develops a culture within the organization that is supportive of security through regular staff awareness and embedding security into daily operations;

c) applies continuous improvement in relation to the effectiveness of security controls and the management of security incidents and in treating security risks in general;

d) embeds security considerations into business processes.

In addition, the organization should maintain reporting on:

e) whether desired security outcomes complied with the requirements of its enterprise protective security architecture;

f) the status or maturity of the organization’s security capability;

g) progress in managing risks to the organization’s assets;

h) significant incidents;

i) effectiveness of security controls;

j) actions taken to ensure the enhancement of controls;

k) third party/external party assurance;

l) compliance reporting requirements;

m) development of organizational security maturity as outlined in Clause 10.

6.2.2.8 Performance monitoring

The organization should monitor the effectiveness of its protective security domains (governance, personnel, information, cyber and physical security) in treating security risks. Regular, frequent and proactive monitoring of risk management processes is essential to maintaining security. Based on assessed risk, the RSE or delegate should determine further treatments in consultation with the asset owner and other relevant interested parties, advise the asset owner accordingly and monitor and report implementation to top management. This is outlined in Figure 9.

Events requiring additional risk assessment can include:

a) changes in protective security policies;

b) new or emerging threats;

c) indications that existing security controls are not effective;

d) identified security gaps and vulnerabilities;

e) security incidents;

f) substantial changes within the operating environment, including but not necessarily limited to changes in systems, technology and the security posture of external interested parties.

NOTE Clause 11 is also relevant to the relationship between effective review and improvement and risk prevention.

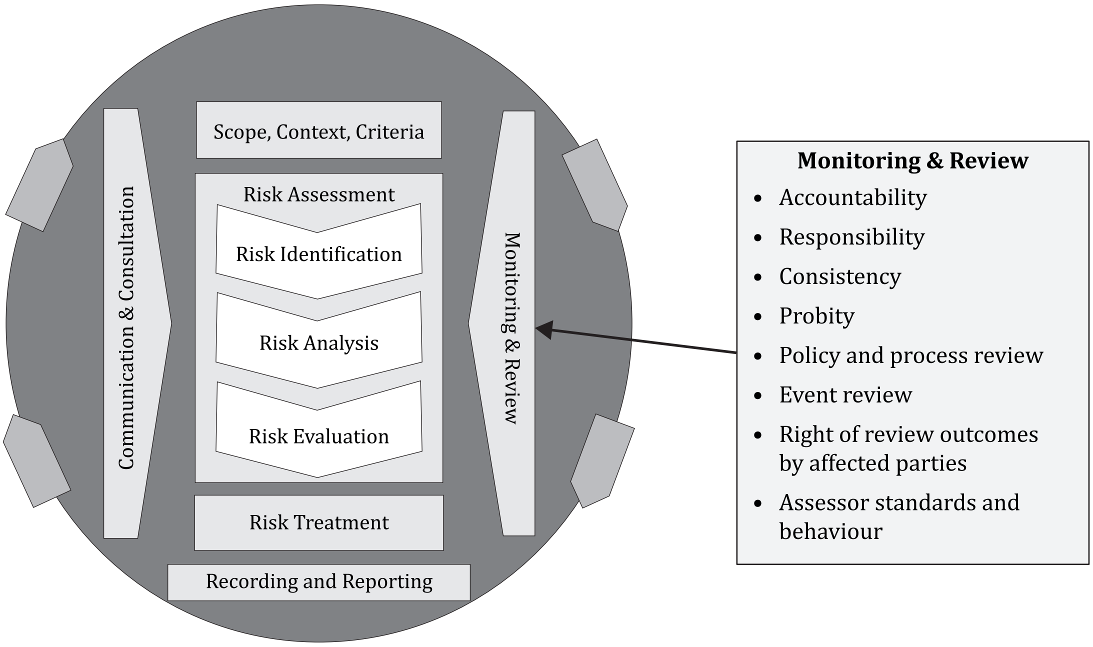


Figure 9 — Security risk management process monitoring and review

6.2.2.9 Service providers and other external or third parties

All service providers should be considered as part of the organization’s security. The organization should ensure contracted service providers are considered in and contribute, as needed, to the risk management process and comply with the security obligations detailed in their contractual or equivalent agreement. Security-related contract provisions should also conform with security policy and procedures.

6.3 Implementation

In implementing the primary security controls that enable delivery of effective security governance, the organization should:

a) formulate and implement organization-wide security governance policy, which should include a statement of principle and an outline of accountability and responsibility at each level of the organization and of the security structure;

b) implement effective oversight and coordination of the organization’s security governance arrangements;

c) manage risk in relation to security governance requirements and organizational objectives;

d) develop and sustain active integration of security within organizational culture;

e) implement organization-wide security risk management;

f) formulate and implement a comprehensive security plan that provides guidance for all aspects of security management;

g) consider application of such approaches as security in depth and deter, detect, delay, respond, recover*;*

h) ensure that those charged with delivering security have the necessary experience and the required qualifications;

i) formulate and deliver security awareness initiatives, including training, which promote awareness across the organization of its security requirements and develop the necessary competence;

j) implement whole-of-organization security incident reporting, management and investigation across the personnel, information, cyber and physical security domains;

k) ensure that security implications are reflected in business continuity, crisis management and disaster recovery planning;

l) implement security arrangements in relation to service providers and contractors;

m) be aware of legal, regulatory and administrative and contractual requirements;

n) formulate, implement and enforce reporting, review and audit of security risk assessments, plans and other arrangements.

The organization should ensure the security governance controls deliver:

o) Accountability: being answerable for decisions and having meaningful mechanisms in place to ensure the organization adheres to all applicable security standards;

p) Transparency: clearly defining roles and responsibilities within the organization for security functions and clear procedures for making decisions and exercising authority;

q) Business value: effectively and efficiently using resources to implement security strategies based on risk management to deliver business objectives;

r) Leadership: achieving an organization-wide commitment to, investment in and sponsorship of, security;

s) Security as core to all aspects of the business: how the organization uses security arrangements to contribute to its overall performance through the secure delivery of its business, while ensuring the confidentiality, integrity and availability of its assets.

7 Personnel security domain

7.1 Objective

In the personnel security domain, the organization should aim to:

- ensure its personnel are eligible, suitable and competent to access sensitive or security classified assets and meet an appropriate standard of integrity and honesty.

The organization should implement controls necessary to provide assurance of the suitability of personnel, contractors and other interested parties to access valuable assets throughout their period of employment or engagement. The following primary risk management controls should be implemented:

a) eligibility and suitability of personnel at recruitment;

b) ongoing assessment of personnel;

c) employment separation;

d) human resource and personnel security management practices.

7.2 Security controls

7.2.1 General

The organization should formulate and apply measures to determine the eligibility and suitability of personnel to have access to its assets. A suitable person demonstrates integrity through honesty, trustworthiness, maturity, resilience and loyalty, and is not vulnerable to improper influence. Effective personnel security facilitates internal and external information sharing and is an essential mitigation strategy in managing the trusted insider threat.

7.2.2 Eligibility and suitability of personnel

The organization should ensure the eligibility and suitability of personnel who have access to sensitive or security classified assets by conducting the relevant screening/checks to provide a level of agreed assurance in accordance with assessed risk.

7.2.3 Ongoing assessment of personnel

The organization should monitor and manage the ongoing suitability of their personnel and, where appropriate, share relevant information of security concern with other organizations and/or authorities.

7.2.4 Separating personnel

The organization should ensure that separating personnel have their access to sensitive or security classified assets promptly withdrawn and are informed of any ongoing security obligations.

7.2.5 Cooperation between human resources and security in applying controls

The organization should ensure that human resources (HR) function is proactively engaged in security and that HR-related information is informing security decision making. Authorized information from human resource areas should be provided to the organization's security authority, if the two are separate. Information that can be relevant includes, but is not necessarily limited to:

a) breaches of the organization's code of conduct;

b) changes in work position;

c) changes in physical work location;

d) changes in compensation status;

e) extended leave arrangements;

f) changes to personal circumstances and life changes that can indicate psychological stress;

g) drug use, including alcohol;

h) criminal history and conduct;

i) attitudes to the workplace;

j) mental health indicators;

k) travel to high-risk places;

l) conflicts of interest.

7.3 Implementation

In implementing the primary security controls that enable delivery of effective personnel security, the organization should:

a) manage personnel security risk;

b) formulate and implement personnel security policy and procedure that encapsulates the full extent of its services;

c) define and implement eligibility and suitability criteria for access to the organization's valuable assets;

d) identify positions or duties that require access to the organization's valuable assets, or which present high risk, and document these requirements e.g. position descriptions;

e) provide one unique identifier for each employee or non-employed service provider;

f) define and implement the organization’s security clearance requirements;

NOTE 1 These can be legal requirements or internally designed to ensure ongoing suitability according to an organization-specific system of access levels.

NOTE 2 This can include appeal arrangements and eligibility exceptions and waivers that can be required from time to time, e.g. in relation to citizenship and checkable background.

g) execute employment screening checks, including eligibility and suitability checks;

h) monitor the ongoing suitability and competence of personnel to access valuable assets, for example through:

- security awareness and training;
- regular security reviews;
- recurring background screening;
- reporting of changes in professional and personal circumstances;
- contact reporting;
- clearance or access level maintenance of contractors;

i) formulate and implement arrangements to manage unsuitable personnel or personnel who are not conforming with security policy;

j) formulate security arrangements in relation to personnel separations;

k) be aware of legal, regulatory and, administrative and contractual requirements;

l) ensure competence by developing and delivering training and awareness programmes to communicate the organization’s security expectations to their personnel and any contractors, suppliers or service providers with access to the organization’s assets;

m) clarify and enforce the responsibilities of external security vetting organizations where these are used;

n) implement policies and procedures for the authorization and withdrawal of temporary or emergency access to sensitive or classified information.

8 Information security domain

8.1 Objective

In the information security domain, the organization should aim to:

- maintain the confidentiality, integrity and availability of the organization’s information.

The organization should implement information security controls necessary to safeguard the organization’s tangible and intangible information, including information that it stores, processes or transmits on behalf of others. Such controls should ensure the appropriate balance between the confidentiality, integrity and availability of the organization’s information and the organization’s risk tolerance. These controls should cover all elements of the information life cycle, from creation, storage, access and transfers to amendments and final disposition (e.g. archival action, destruction).

In delivering the objective of the information security domain, the organization should:

a) identify information holdings, evaluate them according to their business impact and implement controls in proportion to their value, importance and sensitivity;

— This includes evaluation of sensitivity, security classification, handling and storage, disposal and destruction of tangible information, data at rest, data in use and data in transit (cryptographic arrangements, technical standards covering cabling etc.) the physical transfer of tangible information assets (exchange/delivery/receipt of documents etc.) and informal or intangible information exchanges (conversations). The organization should set appropriate priorities regarding confidentiality, integrity and availability according to the level of security risk.

NOTE Further information regarding business impact analysis is available in ISO 22301.

b) enable appropriate access to information according to security clearance and need-to-know, and by controlling access to ICT systems, networks, infrastructure, facilities and equipment;

c) safeguard information.

8.2 Security controls

8.2.1 Business impact and security classification of information

In order to understand business impact and apply security grading/classifications, the organization should evaluate and regularly re-evaluate its information assets throughout the information life cycle, by:

a) developing evaluation criteria to determine business impact levels with a corresponding security classification scheme;

b) identifying and evaluating its information assets (including information shared by other organizations) according to the business impact of reduction or loss of confidentiality, integrity or availability of the information;

c) identifying and evaluating security risks to the inventoried information assets;

d) protecting valuable or sensitive information assets in accordance with perceived business impact of a compromise of their confidentiality, integrity, or availability – information provided by another organization should be protected equivalent to the intent of the originator;

e) implementing operational and technical controls for these information assets proportional to assessed risk (i.e. business impact of reduction or loss of confidentiality, integrity or availability and likelihood of occurrence).

Considerations of sensitivity and protective measures vary according to the business of the organization. A range of criteria are considered by government agencies, such as national security, while many non-government organizations sometimes include a business-related focus on the need to protect valuable intellectual property. In any case, all organizations should limit access to and distribution of information according to the business impact (and likelihood) of reduction or loss of confidentiality, integrity or availability of their sensitive information assets.

8.2.2 Control access to the organization's information

The organization should enable access to proprietary or official information by implementing an identity and access management programme that addresses:

a) sharing information within the organization, in accordance with need-to-know principles, security classification and as reflected in contractual arrangements such as confidentiality agreements;

b) ensuring that any external parties with access to the organization's valuable or sensitive information assets are appropriately cleared by the organization and have a legitimate need-to-know, and that information is shared where it is required for personnel to undertake their duties;

c) controlling access to information.

8.3 Implementation

In implementing the primary security controls that enable delivery of effective information security, the organization should:

a) manage information security risk;

b) formulate and implement enterprise information security policy and procedures as part of organizational security planning, capturing the entire information management life cycle;

c) identify and evaluate information assets and their sensitivity, and assign security classification accordingly;

d) formulate and apply proportionate processes in relation to handling of classified information assets;

e) formulate and apply information sharing processes and agreements between organizations regarding external access;

f) formulate and apply information and digital security incident investigation and management;

g) implement security controls in relation to ICT systems and other digital assets;

h) ensure that security implications are reflected in business continuity and disaster recovery planning.

NOTE 1 Implementing the requirements specified in ISO/IEC 27001 helps organizations meet the requirements in the information security domain.

NOTE 2 ISO/IEC 27002 provides good practice guidelines for controls commonly applied to meet protective security requirements in the information security domain.

9 Cybersecurity domain

9.1 Objective

In the cybersecurity domain the organization should aim to:

— maintain a consistent and secure operating environment that protects it from cyber threats.

The organization should implement controls in four key areas: protection, detection, response and recovery. These controls should be determined and prioritized according to the organization’s evaluation (i.e. the business impact of loss or compromise) of its digital information and related infrastructure, including its information and communications technology systems. The organization’s approach to cybersecurity should be based on risk management. Protecting the organization from a cyber-attack (the deliberate exploitation of computer systems, digitally-dependent enterprise networks and control systems to cause harm) requires security risks and controls to be identified according to accepted risk management principles involving:

a) defining the system;

b) assessing the associated risks;

c) selecting security controls;

d) implementing security controls;

e) reviewing/evaluating/reassessing security controls;

f) authorizing the system;

g) monitoring the system.

9.2 Security controls

9.2.1 Defining the system and selecting security controls

The organization should determine the value of the system and the data and information it processes, stores and communicates in terms of the assessed impact to the organization in the event of loss or compromise. This should be the basis for the design and implementation of security controls in relation to digital systems and for determining the level of acceptable residual risk.

The organization should take an integrated approach to risk analysis and management of complex systems based on the assessed business impact of compromise or loss of systems. This should involve analysis of the organization's reliance on other systems and rigorous documentation of systems. The organization should ensure that the risk to operational networks is assessed and that appropriate risk treatments including levels of segregation to address protection requirements are implemented.

If the organization is handling information arising from the provision or use of operational technology (OT) or industrial control systems (ICS) or is subject in some degree to the security considerations of other organizations, the security considerations of OT, ICS, or the other parties should inform the organization's assessment of business impact and risk.

9.2.2 Implementing and evaluating security controls

The organization should implement security controls in relation to the system and its operating environment based on assessment and management of risk. These controls should be documented in normal risk management practice and system management, and applied as treatments to the specific risks where the degree of application will achieve the desired reduction of likelihood of a negative outcome. The organization should also apply resources consistent with an all-hazards approach to address the risk of unknown and unprecedented secondary and tertiary consequences.

The organization should maintain, evaluate and improve the effectiveness and efficiency of cyber controls as part of its regular security threat and risk monitoring and review activities. In implementing this approach, the organization should not be constrained by a periodic review cycle but should implement a proactive approach to security review, to promote the discovery of unanticipated vulnerabilities and threats to its systems and operating environment. Techniques including, but not limited to, penetration testing, threat assessment and vulnerability assessment should be employed. The security review process should include detailed documentation of findings, including but not necessarily limited to:

a) the assessed security risk regarding the system;

b) the implementation and effectiveness of current security controls;

c) system strengths and weaknesses, and recommended additional controls.

9.2.3 Authorizing cyber systems

The organization should base its decision to implement or authorize a system on the assessed security risks associated with the organization's operation. Risk treatment decisions should be made by asset owners with guidance from the RSE or delegate. Where it is determined that security controls have not been adequately identified or implemented, the RSE should ensure necessary remedial action is undertaken in coordination with the asset owner.

9.2.4 Monitoring cyber systems

Further to 6.2.2.7, the organization should monitor the system and associated cyber threats, security risks and security controls continuously. Based on assessed risk, the RSE should ensure remedial action is undertaken in coordination with the asset owner/top management. Events requiring additional risk assessment can include:

a) changes in security policies relating to the system;

b) new or emerging cyber threats to the system or its operating environment;

c) assessment that existing security controls are not effective;

d) gaps identified by security testing or exercises;

e) a substantial cybersecurity incident involving the system;

f) substantial architectural changes to the system.

9.3 Implementation

In implementing the primary security controls that enable delivery of effective cybersecurity, the organization should:

a) manage cybersecurity risk;

b) implement cybersecurity controls;

c) formulate and implement strategies to protect digital systems from malicious and accidental damage;

d) formulate and implement strategies to limit, detect and recover from cybersecurity incidents;

e) formulate and implement strategies to monitor digital systems to assess the effectiveness of cybersecurity risk treatment and to report cybersecurity status.

NOTE More information relevant to cybersecurity is given in ISO/IEC 27000 and the IEC 62443 series.

9.4 Rapid development of the digital domain

Security issues, whether potential opportunities or threats, and their associated risks, are accentuated by the rapid uptake of technology. Society's growing reliance on technology increases the level and nature of cybersecurity risks.

The organization should monitor and manage the risks arising from changes in its reliance on and adoption of technology. This will require close focus on evolving cybersecurity threats across critical infrastructure and the use of OT for the control and monitoring of physical devices in particular, and the operational integrity of the automation systems themselves. The resilience of an organization and of society in the face of new threat vectors and vulnerabilities resulting from the rapidly expanding scope of networked, digitally-enabled devices is an increasingly important element of security governance, apart from being a critical element of security.

This can be delivered by:

a) safeguarding information assets from cyber threats;

b) maintaining robust business information systems, cyber systems, ICS/OT and data analytics;

c) analysing system and asset dependencies;

d) evaluating downstream impacts on risk;

e) managing network relationships between logical and physical structures.

10 Physical security domain

10.1 Objective

In the physical security domain, the organization should aim to:

— provide a safe and secure physical environment for their assets.

Physical security protects the assets owned or managed by (or entrusted to) the organization. Physical security is an approach based on risk management that utilizes a combination of physical, technological and procedural controls designed to prevent or mitigate physical threats or attacks against people, information and physical assets. The organization should deliver the objective of this domain by implementing protective security controls for the following categories:

a) organizational physical assets;

b) organizational facilities.

These physical security controls should be designed and implemented to mitigate or remove the risk of harm to, or misuse of, its assets.

10.2 Security controls

10.2.1 Organizational physical assets

The organization should:

a) protect its physical assets on the basis of assessed business impact and risk of loss or compromise;

b) on the basis of assessed risk, select appropriate physical security controls to protect the organization's assets and related infrastructure;

c) appropriately and securely dispose of physical assets.

Consistent with this, the treatment from physical security controls should minimize or remove the risk of assets being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorization.

10.2.2 Organizational facilities

The organization should:

a) ensure that security principles, considerations and assessed risk appropriately informs planning, selection, design and modification of buildings and facilities for the protection of assets;

b) identify the areas within its facilities where sensitive or classified information or other valuable assets are used, transmitted, stored or discussed and ensure physical security controls are implemented;

c) identify, equip and if necessary, accredit the areas or zones in which valuable assets are used or stored.

Consistent with this, the organization should ensure security considerations are integrated early in the process of planning, selecting, designing and modifying their facilities. Some governments and industry groups provide detailed guidance on physical security specifications that are relevant to storage of valuable, important or sensitive assets.

10.3 Implementation

In implementing the primary security controls that enable delivery of effective physical security, the organization should:

a) manage physical security risk;

b) formulate and implement the organization's physical security policy, as part of overall organizational security planning;

c) formulate and implement physical security controls to protect the organization's assets by:

- assessing and managing security risks to employees;
- monitoring, recording, analysing and reporting security incidents;

- providing appropriate training and awareness to employees;

d) formulate and implement appropriate physical security controls to protect information assets (including ICT systems), singularly and in aggregation based on business impact level and, if appropriate, classification;

e) determine required assurance levels, e.g. what levels of physical treatment will correspond with levels of assessed security risk;

f) ensure security design principles are incorporated early in planning by:

- applying security in depth principles in relation to facilities, equipment and services;
- including external security controls in overall site planning;
- determining and delineating the areas within the organization where information and assets of various value will be stored;
- undertaking any relevant accreditation and certification requirements;

g) integrate physical security controls into emergency systems and procedures (fire and evacuation, etc.);

h) consider scalable physical security measures ready for activation during increased threat situations;

i) formulate and implement policies and processes for the application of physical security during decommissioning of facilities, equipment and services.

11 Developing the organization’s security maturity

Having implemented an enterprise protective security architecture and framework, the organization should establish approaches for continual improvement and evolving the maturity of its protective security arrangements. This should be undertaken in a manner that considers the organization’s context, purpose and objectives. Where an organization does not have an existing capability maturity model appropriate to its context, the following attributes can be considered in developing a maturity model.

a) Partial

Some primary and supporting security controls of the enterprise protective security architecture are implemented although are not well understood across the organization. Security outcomes are not being achieved in some areas.

Processes are usually ad hoc, informal and undocumented. Some base practices can be performed within the organization, however there is a lack of consistent planning and tracking. Most improvement activity occurs in reaction to incidents rather than proactively. Where practice is good, it reflects the expertise and effort of individuals rather than institutional knowledge. It is possible that some confidence security-related activities are performed adequately, however this performance is variable and the loss of key staff can significantly impact capability and practice.

b) Substantial

The majority of primary and supporting security controls of the enterprise protective security architecture are implemented, broadly managed and understood across the organization. The organization is largely meeting security outcomes.

The importance of security is recognized and key responsibilities are explicitly assigned to positions. At least a base set of protective security measures are planned and tracked. Activities are more repeatable and results more consistent. Policies are documented, but it is possible that processes and procedures are not. Security risks and requirements are occasionally reviewed. Corrective action is usually taken when significant problems are found.

c) Full

All primary and supporting security controls of the enterprise protective security architecture are implemented, integrated into business practices and effectively disseminated across the organization. The organization meets security outcomes.

Policies, processes and standards are well defined and are actively and consistently followed across the organization. Governance and management structures are in place. Risk assessment and management activities are regularly scheduled and completed. Historic performance information is periodically assessed and used to determine where improvements should be made.

d) Excelled

All primary and supporting security controls of the enterprise protective security architecture are effectively integrated and exceeding security outcomes with better-practice guidance achieving high performance.

The organization adapts dynamically and automatically in response to situational changes. Quantitative performance measures are defined, baselined and applied to ensure security performance is analysed objectively and can be accurately predicted in advance. The organization implements many optional "better practice" requirements in response to its risk assessment. Security is a strategic issue for the organization. Long-term planning is in place and integrated with business planning to predict and prepare for protective security challenges. Effective continuous process improvement is operating, supported by real time, metrics-based performance data. Mechanisms are also in place to encourage, develop and test innovations.

As reflected in Table 2, attributes should be applied to each of the security controls/risk treatments in the five security domains:

i) Security governance (6.3)

ii) Personnel security (7.3)

iii) Information security (8.3)

iv) Cybersecurity (9.3)

v) Physical security (10.3).

Table 2 — Maturity model template

	Partial	Substantial	Full	Excelled
	Some primary and supporting security controls of the enterprise protective security architecture are implemented although are not well understood across the organization. Security outcomes are not being achieved in some areas.	The majority of primary and supporting security controls of the enterprise protective security architecture are implemented, broadly managed and understood across the organization. The organization is largely meeting security outcomes.	All primary and supporting security controls of the enterprise protective security architecture are implemented, integrated into business practices and effectively disseminated across the organization. The organization meets security outcomes.	All primary and supporting security controls of the enterprise protective security architecture are effectively integrated and exceeding security outcomes with better-practice guidance achieving high performance.
Security Governance				
Personnel Security				
Information Security				
Cyber Security				
Physical Security				

Bibliography

[1] ISO 22301, *Security and resilience — Business continuity management systems — Requirements*

[2] ISO/IEC/TR 23188:2020, *Information technology — Cloud computing — Edge computing landscape*

[3] ISO/IEC 27000:2018, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

[4] ISO/IEC 27001, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*

[5] ISO/IEC 27002, *Information security, cybersecurity and privacy protection — Information security controls*

[6] ISO/IEC 30071-1:2019, *Information technology — Development of user interface accessibility — Part 1: Code of practice for creating accessible ICT products and services*

[7] ISO 31000:2018, *Risk management — Guidelines*

[8] IEC 31010, *Risk management — Risk assessment techniques*

[9] ISO/IEC Guide 51:2014, *Safety aspects — Guidelines for their inclusion in standards*

[10] ISO/IEC Guide 63:2019, *Guide to the development and inclusion of aspects of safety in International Standards for medical devices*

[11] IEC 62443 (all parts), *Industrial communication networks - Network and system security*

ICS 03.100.01; 13.310

Price based on 31 pages

iso.org