INTERNATIONAL STANDARD

ISO 28000

Second edition
2022-03

Security and resilience — Security management systems — Requirements

Reference number
ISO 28000:2022(E)

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

Page

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 documents 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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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.*

This second edition cancels and replaces the first edition (ISO 28000:2007), which has been technically revised, but maintains existing requirements to provide continuity for organizations using the previous edition. The main changes are as follows:

— recommendations on principles have been added in Clause 4 to give better coordination with ISO 31000;

— recommendations have been added in Clause 8 for better consistency with ISO 22301, facilitating integration including:

  — security strategies, procedures, processes and treatments;

  — security plans.

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

Most organizations are experiencing an increasing uncertainty and volatility in the security environment. As a consequence, they face security issues that impact on their objectives, which they want to address systematically within their management system. A formal approach to security management can contribute directly to the business capability and credibility of the organization.

This document specifies requirements for a security management system, including those aspects critical to the security assurance of the supply chain. It requires the organization to:

— assess the security environment in which it operates including its supply chain (including dependencies and interdependencies);

— determine if adequate security measures are in place to effectively manage security-related risks;

— manage compliance with statutory, regulatory and voluntary obligations to which the organization subscribes;

— align security processes and controls, including the relevant upstream and downstream processes and controls of the supply chain to meet the organization's objectives.

Security management is linked to many aspects of business management. They include all activities controlled or influenced by organizations, including but not limited to those that impact on the supply chain. All activities, functions and operations should be considered that have an impact on the security management of the organization including (but not limited to) its supply chain.

With regard to the supply chain, it has to be considered that supply chains are dynamic in nature. Therefore, some organizations managing multiple supply chains may look to their providers to meet related security standards as a condition of being included in that supply chain in order to meet requirements for security management.

This document applies the Plan-Do-Check-Act (PDCA) model to planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving the effectiveness of an organization's security management system, see Table 1 and Figure 1.

Table 1 — Explanation of the PDCA model

Plan (Establish)	Establish security policy, objectives, targets, controls, processes and procedures relevant to improving security in order to deliver results that align with the organization's overall policies and objectives.
Do (Implement and operate)	Implement and operate the security policy, controls, processes and procedures.
Check (Monitor and review)	Monitor and review performance against security policy and objectives, report the results to management for review, and determine and authorize actions for remediation and improvement.
Act (Maintain and improve)	Maintain and improve the security management system by taking corrective action, based on the results of management review and reappraising the scope of the security management system and security policy and objectives.

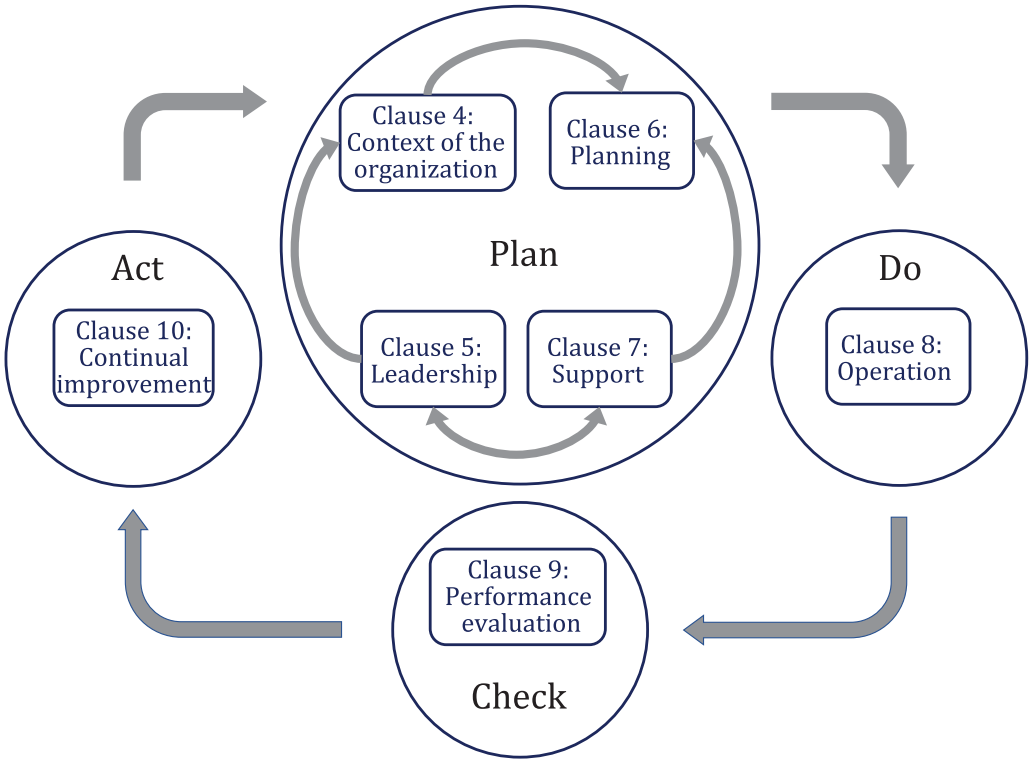

Figure 1 — PDCA model applied to the security management system

This ensures a degree of consistency with other management system standards, such as ISO 9001, ISO 14001, ISO 22301, ISO/IEC 27001, ISO 45001, etc., thereby supporting consistent and integrated implementation and operation with related management systems.

For organizations that so wish, conformity of the security management system to this document may be verified by an external or internal auditing process.

Security and resilience — Security management systems — Requirements

1 Scope

This document specifies requirements for a security management system, including aspects relevant to the supply chain.

This document is applicable to all types and sizes of organizations (e.g. commercial enterprises, government or other public agencies and non-profit organizations) which intend to establish, implement, maintain and improve a security management system. It provides a holistic and common approach and is not industry or sector specific.

This document can be used throughout the life of the organization and can be applied to any activity, internal or external, at all levels.

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 terminological 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
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its *objectives* (3.7)

Note 1 to entry: The concept of organization includes, but is not limited to, sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

Note 2 to entry: If the organization is part of a larger entity, the term "organization" refers only to the part of the larger entity that is within the scope of the *security management system* (3.5).

3.2
interested party (preferred term)
stakeholder (admitted term)
person or *organization* (3.1) that can affect, be affected by, or perceive itself to be affected by a decision or activity

3.3
top management
person or group of people who directs and controls an *organization* (3.1) at the highest level

Note 1 to entry: Top management has the power to delegate authority and provide resources within the organization.

Note 2 to entry: If the scope of the *management system* (3.4) covers only part of an organization, then top management refers to those who direct and control that part of the organization.

3.4
management system
set of interrelated or interacting elements of an *organization* (3.1) to establish *policies* (3.6) and *objectives* (3.7), as well as *processes* (3.9) to achieve those objectives

Note 1 to entry: A management system can address a single discipline or several disciplines.

Note 2 to entry: The management system elements include the organization's structure, roles and responsibilities, planning and operation.

3.5
security management system
system of coordinated *policies* (3.6), *processes* (3.9) and practices through which an organization manages its security *objectives* (3.7)

3.6
policy
intentions and direction of an *organization* (3.1) as formally expressed by its *top management* (3.3)

3.7
objective
result to be achieved

Note 1 to entry: An objective can be strategic, tactical, or operational.

Note 2 to entry: Objectives can relate to different disciplines (such as finance, health and safety, and environment). They can be, for example, organization-wide or specific to a project, product and *process* (3.9).

Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended result, as a purpose, as an operational criterion, as a security objective, or by the use of other words with similar meaning (e.g. aim, goal, or target).

Note 4 to entry: In the context of *security management systems* (3.5), security objectives are set by the *organization* (3.1), consistent with the security *policy* (3.6), to achieve specific results.

3.8
risk
effect of uncertainty on *objectives* (3.7)

Note 1 to entry: An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.

Note 2 to entry: Objectives can have different aspects and categories, and can be applied at different levels.

Note 3 to entry: Risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood.

3.9
process
set of interrelated or interacting activities that uses or transforms inputs to deliver a result

Note 1 to entry: Whether the result of a process is called an output, a product or a service depends on the context of the reference.

3.10
competence
ability to apply knowledge and skills to achieve intended results

3.11
documented information
information required to be controlled and maintained by an *organization* (3.1) and the medium on which it is contained

Note 1 to entry: Documented information can be in any format and media, and from any source.

Note 2 to entry: Documented information can refer to:

— the *management system* (3.4), including related *processes* (3.9);

— information created in order for the organization to operate (documentation);

— evidence of results achieved (records).

3.12
performance
measurable result

Note 1 to entry: Performance can relate either to quantitative or qualitative findings.

Note 2 to entry: Performance can relate to managing activities, *processes* (3.9), products, services, systems or *organizations* (3.1).

3.13
continual improvement
recurring activity to enhance *performance* (3.12)

3.14
effectiveness
extent to which planned activities are realized and planned results are achieved

3.15
requirement
need or expectation that is stated, generally implied or obligatory

Note 1 to entry: "Generally implied" means that it is custom or common practice for the *organization* (3.1) and *interested parties* (3.2) that the need or expectation under consideration is implied.

Note 2 to entry: A specified requirement is one that is stated, e.g. in *documented information* (3.11).

3.16
conformity
fulfilment of a *requirement* (3.15)

3.17
nonconformity
non-fulfilment of a *requirement* (3.15)

3.18
corrective action
action to eliminate the cause(s) of a *nonconformity* (3.17) and to prevent recurrence

3.19
audit
systematic and independent *process* (3.9) for obtaining evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

Note 1 to entry: An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines).

Note 2 to entry: An internal audit is conducted by the *organization* (3.1) itself, or by an external party on its behalf.

Note 3 to entry: "Audit evidence" and "audit criteria" are defined in ISO 19011.

3.20
measurement
process (3.9) to determine a value

3.21
monitoring
determining the status of a system, a *process* (3.9) or an activity

Note 1 to entry: To determine the status, there can be a need to check, supervise or critically observe.

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 result(s) of its security management system including the requirements of its supply chain.

4.2 Understanding the needs and expectations of interested parties

4.2.1 General

The organization shall determine:

— the interested parties that are relevant to the security management system;

— the relevant requirements of these interested parties;

— which of these requirements will be addressed through the security management system.

4.2.2 Legal, regulatory and other requirements

The organization shall:

a) implement and maintain a process to identify, have access to and assess the applicable legal, regulatory and other requirements related to its security;

b) ensure that these applicable legal, regulatory and other requirements are taken into account in implementing and maintaining its security management system;

c) document this information and keep it up to date;

d) communicate this information to relevant interested parties as appropriate.

4.2.3 Principles

4.2.3.1 General

The purpose of security management within the organization is the creation and, in particular, the protection of value.

The organization should apply the principles given in Figure 2 and described in 4.2.3.2 to 4.2.3.9.

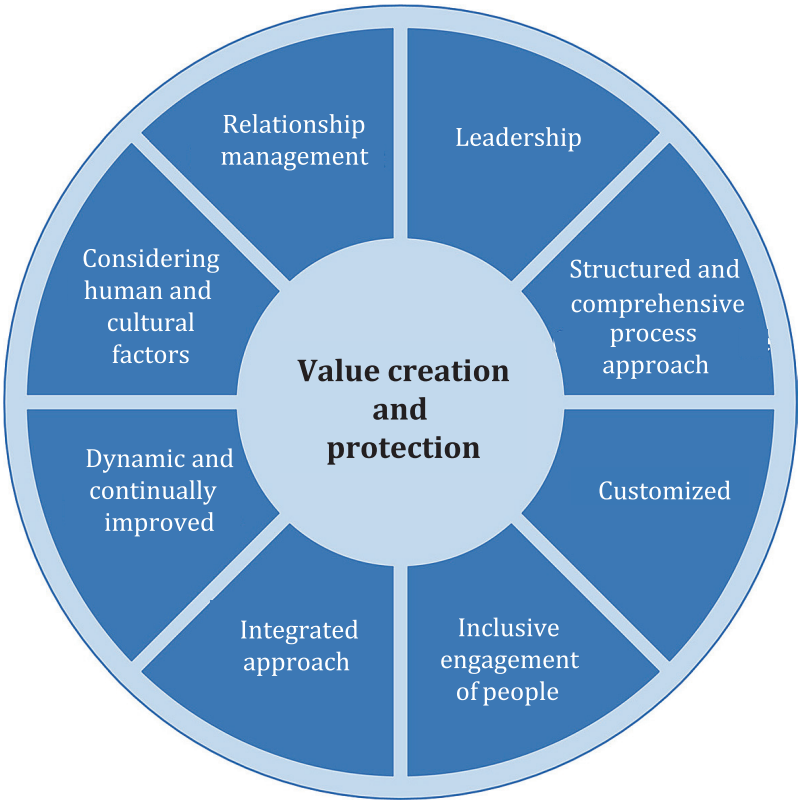

Figure 2 — Principles

4.2.3.2 Leadership

Leaders at all levels should establish unity of purpose and direction. They should create conditions to align the organization's strategies, policies processes and resources to achieve its objectives. Clause 5 explains the requirements with regard to this principle.

4.2.3.3 Structured and comprehensive process approach based on best available information

A structured and comprehensive approach to security management including the supply chain should contribute to consistent and comparable results, which are achieved more effectively and efficiently when activities are understood and managed as interrelated processes functioning as a coherent system.

4.2.3.4 Customized

The security management system should be customized and proportionate to the organization's external and internal context and needs. It should be related to its objectives.

4.2.3.5 Inclusive engagement of people

The organization should involve interested parties appropriately and in a timely manner. It should consider their knowledge, views and perceptions appropriately to improve awareness of and facilitate informed security management. The organization should ensure that everybody at all levels is respected and involved.

4.2.3.6 Integrated approach

Security management is an integral part of all organizational activities. It should be integrated with all other management systems of the organization.

The organization's risk management – whether formal, informal or intuitive – should be integrated into the security management system.

4.2.3.7 Dynamic and continually improved

The organization should have an ongoing focus on improvement through learning and experience to maintain the level of performance, to react to changes and to create new opportunities as the external and internal context of the organization changes.

4.2.3.8 Considering human and cultural factors

Human behaviour and culture significantly influence all aspects of security management and should be considered at each level and stage. Decisions should be based on the analysis and evaluation of data and information to ensure they result in greater objectivity, confidence in decision-making and are more likely to produce desired results. Individual perceptions should be considered.

4.2.3.9 Relationship management

For sustained success, the organization should manage its relationships with all relevant interested parties as they might influence the performance of the organization.

4.3 Determining the scope of the security management system

The organization shall determine the boundaries and applicability of the security management system to establish its scope.

When determining this scope, the organization shall consider:

— the external and internal issues referred to in 4.1;

— the requirements referred to in 4.2.

The scope shall be available as documented information.

Where an organization chooses to have any process that affects conformity with its security management system externally provided, the organization shall ensure that such processes are controlled. The necessary controls for and responsibilities of such externally provided processes shall be identified within the security management system.

4.4 Security management system

The organization shall establish, implement, maintain and continually improve a 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 security management system by:

— ensuring that the security policy and security objectives are established and are compatible with the strategic direction of the organization;

— ensuring that the requirements and expectations of the organization's interested parties are identified and monitored, and appropriate timely action is taken to manage these expectations to ensure the integration of the security management system requirements into the organization's business processes;

— ensuring the integration of the security management system requirements into the organization's business processes;

— ensuring that the resources needed for the security management system are available;

— communicating the importance of effective security management and of conforming to the security management system requirements;

— ensuring that the security management system achieves its intended result(s);

— ensuring the viability of the security management objectives, targets and programmes;

— ensuring any security programmes generated from other parts of the organization complement the security management system;

— directing and supporting persons to contribute to the effectiveness of the security management system;

— promoting continual improvement of the organization's security management system;

— supporting other relevant 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 Security policy

5.2.1 Establishing the security policy

Top management shall establish a security policy that:

a) is appropriate to the purpose of the organization;

b) provides a framework for setting security objectives;

c) includes a commitment to meet applicable requirements;

d) includes a commitment to continual improvement of the security management system;

e) considers the adverse impact that the security policy, objectives, targets, programmes, etc. can have on other aspects of the organization.

5.2.2 Security policy requirements

The security policy shall:

— be consistent with other organizational policies;

— be consistent with the organization's overall security risk assessment;

— provide for its review in case of the acquisition of, or a merger with, other organizations, or other changes to the business scope of the organization which could affect the continuity or relevance of the security management system;

— describe and allocate primary accountability and responsibility for outcomes;

— be available as documented information;

— be communicated within the organization;

— be available to interested parties, as appropriate.

NOTE Organizations can choose to have a detailed security management policy for internal use which would provide sufficient information and direction to drive the security management system (parts of which can be confidential) and have a summarized (non-confidential) version containing the broad objectives for dissemination to their interested parties.

5.3 Roles, responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the organization.

Top management shall assign the responsibility and authority for:

a) ensuring that the security management system conforms to the requirements of this document;

b) reporting on the performance of the security management system to top management.

6 Planning

6.1 Actions to address risks and opportunities

6.1.1 General

When planning for the 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:

— give assurance that the security management system can achieve its intended result(s);

— prevent, or reduce, undesired effects;

— achieve continual improvement.

The organization shall plan:

a) actions to address these risks and opportunities;

b) how to:

— integrate and implement the actions into its security management system processes;

— evaluate the effectiveness of these actions.

The purpose of managing risks is the creation and protection of value. Managing risk shall be integrated into the security management system. Risks related to the security of the organization and its interested parties are addressed in 8.3.

6.1.2 Determining security-related risks and identifying opportunities

Determining security-related risks and identifying and exploiting opportunities requires a proactive risk assessment which shall include consideration of, but not be limited to:

a) physical or functional failures and malicious or criminal acts;

b) environmental, human and cultural factors and other internal or external contexts, including factors outside the organization's control affecting the organization's security;

c) the design, installation, maintenance and replacement of security equipment;

d) the organization's information, data, knowledge and communication management;

e) information related to security threats and vulnerabilities;

f) the interdependencies between suppliers.

6.1.3 Addressing security-related risks and exploiting opportunities

The evaluation of the identified security-related risk shall provide input to (but not be limited to):

a) the organization's overall risk management;

b) risk treatment;

c) security management objectives;

d) security management processes;

e) the design, specification and implementation of the security management system;

f) the identification of adequate resources including staffing;

g) the identification of training needs and the required level of competence.

6.2 Security objectives and planning to achieve them

6.2.1 Establishing security objectives

The organization shall establish security objectives at relevant functions and levels.

The security objectives shall:

a) be consistent with the security policy;

b) be measurable (if practicable);

c) take into account applicable requirements;

d) be monitored;

e) be communicated;

f) be updated as appropriate;

g) be available as documented information.

6.2.2 Determining security objectives

When planning how to achieve its security objectives, the organization shall determine:

— what will be done;

— what resources will be required;

— who will be responsible;

— when it will be completed;

— how the results will be evaluated.

When establishing and reviewing its security objectives, an organization shall take into account:

a) technological, human, administrative and other options;

b) views of and impacts on appropriate interested parties.

The security objectives shall be consistent with the organization's commitment to continual improvement.

6.3 Planning of changes

When the organization determines the need for changes to the security management system, including those identified in Clause 10, the changes shall be carried out in a planned manner.

The organization shall consider:

a) the purpose of the changes and their potential consequences;

b) the integrity of the security management system;

c) the availability of resources;

d) the allocation or reallocation of responsibilities and authorities.

7 Support

7.1 Resources

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

7.2 Competence

The organization shall:

— determine the necessary competence of person(s) doing work under its control that affects its security performance;

— ensure that these persons are competent on the basis of appropriate education, training, or experience and are appropriately security cleared;

— where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken;

Appropriate documented information shall be available as evidence of competence.

NOTE Applicable actions can include, for example: the provision of training to, the mentoring of, or the reassignment of currently employed persons; or the hiring or contracting of competent persons.

7.3 Awareness

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

— the security policy;

— their contribution to the effectiveness of the security management system, including the benefits of improved security performance;

— the implications of not conforming with the security management system requirements;

— their roles and responsibilities in achieving compliance with the security management policy and procedures and with the requirements of the security management system, including emergency preparedness and response requirements.

7.4 Communication

The organization shall determine the internal and external communications relevant to the security management system, including:

— on what it will communicate;

— when to communicate;

— with whom to communicate;

— how to communicate;

— the sensitivity of information prior to dissemination.

7.5 Documented information

7.5.1 General

The organization's security management system shall include:

a) documented information required by this document;

b) documented information determined by the organization as being necessary for the effectiveness of the security management system.

The documented information shall describe the responsibilities and authorities for achieving security management objectives and targets, including the means and timelines to achieve those objectives and targets.

NOTE The extent of documented information for a security management system can differ from one organization to another due to:

— the size of organization and its type of activities, processes, products and services;

— the complexity of processes and their interactions;

— the competence of persons.

The organization shall determine the value of information, and establish the level of integrity required and the security controls to prevent unauthorized access.

7.5.2 Creating and updating documented information

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

— identification and description (e.g. a title, date, author, or reference number);

— format (e.g. language, software version, graphics) and media (e.g. paper, electronic);

— review and approval for suitability and adequacy.

7.5.3 Control of documented information

Documented information required by the 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;

b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity);

c) it is periodically reviewed and revised as necessary, and approved for adequacy by authorized personnel;

d) obsolete documents, data and information are promptly removed from all points of issue and points of use, or otherwise assured against unintended use;

e) archival documents, data and information retained for legal or knowledge preservation purposes or both are suitably identified.

For the control of documented information, the organization shall address the following activities, as applicable:

— distribution, access, retrieval and use;

— storage and preservation, including preservation of legibility;

— control of changes (e.g. version control);

— retention and disposition.

Documented information of external origin determined by the organization to be necessary for the planning and operation of the 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.

8 Operation

8.1 Operational planning and control

The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Clause 6, by:

— establishing criteria for the processes;

— implementing control of the processes in accordance with the criteria.

Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned.

8.2 Identification of processes and activities

The organization shall identify those processes and activities that are necessary for achieving:

a) compliance with its security policy;

b) compliance with legal, statutory and regulatory security requirements;

c) its security management objectives;

d) the delivery of its security management system;

e) the required level of security of the supply chain.

8.3 Risk assessment and treatment

The organization shall implement and maintain a risk assessment and treatment process.

NOTE The process for risk assessment and treatment is addressed in ISO 31000.

The organization should:

a) identify its security-related risks, prioritizing them to the resources required for its security management;

b) analyse and evaluate the identified risks;

c) determine which risks require treatment;

d) select and implement options to address those risks;

e) prepare and implement risk treatment plans.

NOTE Risks in this subclause relate to the security of the organization and its interested parties. Risks and opportunities related to the effectiveness of the management system are addressed in 6.1.

8.4 Controls

The processes listed in 8.2 shall include controls for human resource management, as well as the design, installation, operation, refurbishment and modification of security-related items of equipment, instrumentation and information technology, as appropriate. Where existing arrangements are revised or new arrangements introduced that could have impact on security management, the organization shall consider the associated security-related risks before their implementation. The new or revised arrangements to be considered shall include:

a) revised organizational structure, roles or responsibilities;

b) training, awareness and human resource management;

c) revised security management policy, objectives, targets or programmes;

d) revised processes and procedures;

e) the introduction of new infrastructure, security equipment or technology, which may include hardware and/or software;

f) the introduction of new contractors, suppliers or personnel, as appropriate;

g) the requirements for security assurance of external suppliers.

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that externally provided processes, products or services that are relevant to the security management system are controlled.

8.5 Security strategies, procedures, processes and treatments

8.5.1 Identification and selection of strategies and treatments

The organization should implement and maintain systematic processes for analysing vulnerabilities and threats related to security. Based on this vulnerability and threat analysis and consequent risk assessment, the organization should identify and select a security strategy which comprises one or more procedures, processes and treatments.

Identification should be based on the extent to which strategies, procedures, processes and treatments:

a) maintain the organization's security;

b) reduce the likelihood of security vulnerability;

c) reduce the likelihood of a threat being actualised;

d) shorten the period of any security treatment deficiencies and limit their impact;

e) provide for the availability of adequate resources.

Selection should be based on the extent to which strategies, processes and treatments:

— meet the requirements to protect the organization's security;

— consider the amount and type of risk the organization may or may not take;

— consider the associated costs and benefits.

8.5.2 Resource requirements

The organization shall determine the resource requirements to implement the selected security procedures, processes and treatments.

8.5.3 Implementation of treatments

The organization shall implement and maintain selected security treatments.

8.6 Security plans

8.6.1 General

The organization shall establish and document security plans and procedures based on the selected strategies and treatments. The organization shall implement and maintain a response structure that will enable timely and effective warning and communication of vulnerabilities related to security and imminent security threats or ongoing security violations to relevant interested parties. The response structure shall provide plans and procedures to manage the organization during an imminent security threat or an ongoing security violation.

8.6.2 Response structure

The organization shall implement and maintain a structure, identifying a designated person or one or more teams responsible for responding to vulnerabilities and threats related to security. The roles and responsibilities for the designated person or each team and the relationship between the person or teams shall be clearly identified, communicated and documented.

Collectively, the teams should be competent to:

a) assess the nature and extent of a security threat and its potential impact;

b) assess the impact against pre-defined thresholds that justify initiation of a formal response;

c) activate an appropriate security response;

d) plan actions that need to be undertaken;

e) establish priorities using life safety as the first priority;

f) monitor the effects of any variation in vulnerabilities related to security, changes to the intent and capability of threat actors or security violations and the organization's response;

g) activate the security treatments;

h) communicate with relevant interested parties, authorities and the media;

i) contribute to a communication plan with communication management.

For each designated person or team there should be:

— identified staff, including alternates with the necessary responsibility, authority and competence to perform their designated role;

— documented procedures to guide their actions including those for the activation, operation, coordination and communication of the response.

8.6.3 Warning and communication

The organization should document and maintain procedures for:

a) communicating internally and externally to relevant interested parties, including what, when, with whom and how to communicate;

NOTE The organization can document and maintain procedures for how, and under what circumstances, the organization communicates with employees and their emergency contacts.

b) receiving, documenting and responding to communications from interested parties, including any national or regional risk advisory system or equivalent;

c) ensuring the availability of the means of communication during a security violation, vulnerability or threat;

d) facilitating structured communication with responders to security threats and/or violations;

e) providing details of the organization's media response following a security violation, including a communications strategy;

f) recording the details of the security violation, the actions taken and the decisions made.

Where applicable, the following should also be considered and implemented:

— alerting interested parties potentially impacted by an actual or impending security violation;

— ensuring appropriate coordination and communication between multiple responding organizations.

The warning and communication procedures shall be exercised as part of the organization's testing and training programme.

8.6.4 Content of the security plans

The organization shall document and maintain security plans. Those plans should provide guidance and information to assist teams to respond to a security vulnerability, threat and/or violation and to assist the organization with the response and restoring its security.

Collectively, security plans should contain:

a) details of the actions that the teams will take to:

   1) continue or restore the agreed security status;

   2) monitor the impact of the actual or impending security threats, vulnerabilities or violation and the organization's response to it;

b) reference to the pre-defined threshold(s) and process for activating the response;

c) procedures to restore the security of the organization;

d) details to manage the immediate consequences of a security vulnerability and threat or actual or impending security violation giving due regard to:

   1) the welfare of individuals;

   2) the value of the assets, information and personnel potentially compromised;

   3) the prevention of (further) loss or unavailability of core activities.

Each plan should include:

— its purpose, scope and objectives;

— the roles and responsibilities of the team that will implement the plan;

— the actions to implement the solutions;

— the information needed to activate (including activation criteria), operate, coordinate and communicate the team's actions;

— internal and external interdependencies;

— its resource requirements;

— its reporting requirements;

— a process for standing down.

Each plan should be usable and available at the time and place at which it is required.

8.6.5 Recovery

The organization shall have documented processes to restore the organization's security from any temporary measures adopted before, during and after a security violation.

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

The organization shall determine:

— what needs to be monitored and measured;

— the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;

— when the monitoring and measuring shall be performed;

— when the results from monitoring and measurement shall be analysed and evaluated.

Documented information shall be available as evidence of the results.

The organization shall evaluate the performance and the effectiveness of the security management system.

9.2 Internal audit

9.2.1 General

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

a) conforms to:

   1) the organization's own requirements for its security management system;

   2) the requirements of this document;

b) is effectively implemented and maintained.

9.2.2 Internal audit programme

The organization shall plan, establish, implement and maintain (an) audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting.

When establishing the internal audit programme(s), the organization shall consider the importance of the processes concerned and the results of previous audits.

The organization shall:

a) define the audit objectives, criteria and scope for each audit;

b) select auditors and conduct audits to ensure objectivity and the impartiality of the audit process;

c) ensure that the results of the audits are reported to relevant managers.

d) verify that the security equipment and personnel are appropriately deployed;

e) ensure that any necessary corrective actions are taken without undue delay to eliminate detected nonconformities and their causes;

f) ensure that follow-up audit actions include the verification of the actions taken and the reporting of verification results.

Documented information shall be available as evidence of the implementation of the audit programme(s) and the audit results.

The audit programme, including any schedule, shall be based on the results of risk assessments of the organization's activities and the results of previous audits. The audit procedures shall cover the scope, frequency, methodologies and competencies, as well as the responsibilities and requirements for conducting audits and reporting results.

9.3 Management review

9.3.1 General

Top management shall review the organization's security management system, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness.

The organization shall consider the results of analysis and evaluation, and the outputs from management review, to determine if there are needs or opportunities relating to the business or to the security management system that shall be addressed as part of continual improvement.

NOTE The organization can use the processes of the security management system, such as leadership, planning and performance evaluation, to achieve improvement.

9.3.2 Management review inputs

The management review shall include:

a) the status of actions from previous management reviews;

b) changes in external and internal issues that are relevant to the security management system;

c) changes in needs and expectations of interested parties that are relevant to the security management system;

d) information on the security performance, including trends in:

   1) nonconformities and corrective actions;

   2) monitoring and measurement results;

   3) audit results;

e) opportunities for continual improvement;

f) results of audits and evaluations of compliance with legal requirements and other requirements to which the organization subscribes;

g) communication(s) from external interested parties, including complaints;

h) the security performance of the organization;

i) the extent to which objectives and targets have been met;

j) status of corrective actions;

k) follow-up actions from previous management reviews;

l) changing circumstances, including developments to legal, regulatory and other requirements (see 4.2.2) related to security aspects;

m) recommendations for improvement.

9.3.3 Management review results

The results of the management review shall include decisions related to continual improvement opportunities and any need for changes to the security management system.

Documented information shall be available as evidence of the results of management reviews.

10 Improvement

10.1 Continual improvement

The organization shall continually improve the suitability, adequacy and effectiveness of the security management system. The organization should actively seek opportunities for improvement, even if not prompted by vulnerabilities related to security and imminent security threats or ongoing security violations to relevant interested parties.

10.2 Nonconformity and corrective action

When a nonconformity occurs, the organization shall:

a) react to the nonconformity, and as applicable:

   1) take action to control and correct it;

   2) deal with the consequences;

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

   1) reviewing the nonconformity;

   2) determining the causes of the nonconformity;

   3) determining if similar nonconformities exist, or can potentially occur;

c) implement any action needed;

d) review the effectiveness of any corrective action taken;

e) make changes to the security management system, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered.

Documented information shall be available as evidence of:

— the nature of the nonconformities and any subsequent actions taken;

— the results of any corrective action;

— the investigation of security-related:

   — failures, including near misses and false alarms;

   — incidents and emergency situations;

   — nonconformities;

— taking action to mitigate any consequences arising from such failures, incidents or nonconformities.

Procedures shall require that all proposed corrective actions are reviewed through the assessment process of security-related risk prior to implementation unless immediate implementation forestalls imminent exposures to life or public safety.

Any corrective action taken to eliminate the causes of actual and potential nonconformities shall be appropriate to the magnitude of the problems and commensurate with the security-management-related risks likely to be encountered.

Bibliography

[1] ISO 9001, *Quality management systems — Requirements*

[2] ISO 14001, *Environmental management systems — Requirements with guidance for use*

[3] ISO 19011, *Guidelines for auditing management systems*

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

[5] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[6] ISO 28001, *Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance*

[7] ISO 28002, *Security management systems for the supply chain — Development of resilience in the supply chain — Requirements with guidance for use*

[8] ISO 28003, *Security management systems for the supply chain — Requirements for bodies providing audit and certification of supply chain security management systems*

[9] ISO 28004-1, *Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 1: General principles*

[10] ISO 28004-3, *Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 3: Additional specific guidance for adopting ISO 28000 for use by medium and small businesses (other than marine ports)*

[11] ISO 28004-4, *Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 4: Additional specific guidance on implementing ISO 28000 if compliance with ISO 28001 is a management objective*

[12] ISO 31000, *Risk management — Guidelines*

[13] ISO 45001, *Occupational health and safety management systems — Requirements with guidance for use*

[14] ISO Guide 73, *Risk management — Vocabulary*

ICS 03.100.01; 03.100.70

Price based on 20 pages