DRAFT INTERNATIONAL STANDARD

ISO/DIS 28000

ISO/TC **292** Secretariat: **SIS**

Voting begins on:
2021-02-23

Voting terminates on:
2021-05-18

Security and resilience - Security management systems – Requirements for the supply chain

ICS: 03.100.01; 03.100.70

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.

Reference number
ISO/DIS 28000:2021(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 compared with the previous edition are as follows:

— ISO directives Annex L, Appendix 2 has been followed

— 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:

  o security strategies, procedures, processes and treatments,

  o security plans

A list of all parts in the ISO 28000 series can be found on the ISO website.

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

There is an increasing uncertainty and volatility in the security environment experienced by most organizations. As a consequence, they face security issues impacting on their objectives and want to address them 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 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; and,
- Align security processes and controls, including the relevant upstream and downstream processes and controls of the supply chain to meet the organization’s objectives.

It requires the organization to assess the security environment in which it operates and to determine if adequate security measures are in place to effectively manage security related risks and if other regulatory security related requirements already exist with which the organization complies.

If security objectives are identified, the organization implements controls to meet these 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.

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 (SMS) by taking corrective action, based on the results of management review and reappraising the scope of the SMS and security policy and objectives.

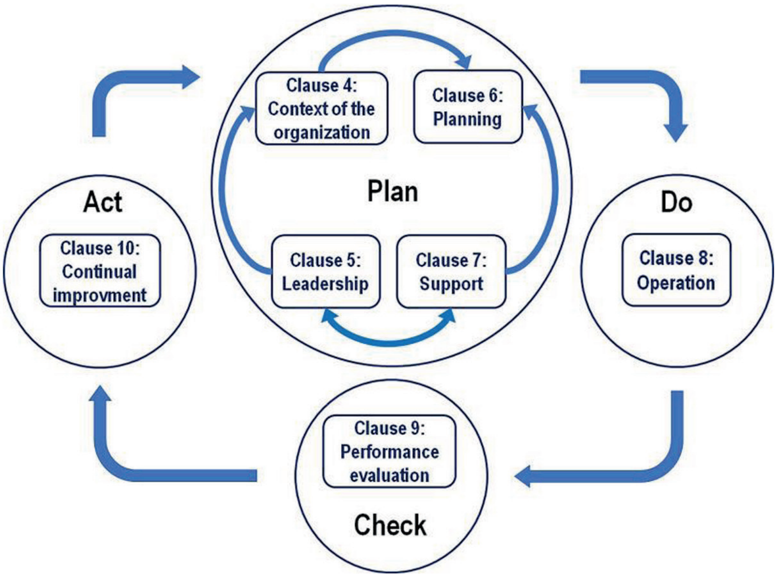
Plan
Clause 4: Context of the organization
Clause 6: Planning
Clause 5: Leadership
Clause 7: Support
Do
Clause 8: Operation
Check
Clause 9: Performance evaluation
Act
Clause 10: Continual improvment

Figure 1 — PDCA model applied to the security management system

This ensures a degree of consistency with other management systems standards, such as ISO 9001, Quality management systems – Requirements, ISO 14001, Environmental management systems - Requirements with guidance for use, ISO 22301, Security and resilience - Business continuity management systems – Requirements, ISO/IEC 27001, Information technology - Security techniques - Information security management systems – Requirement, ISO 45001, Occupational health and safety management systems - Requirements with guidance for use, etc. thereby supporting consistent and integrated implementation and operation with related management systems.

Compliance with an International Standard does not in itself confer immunity from legal obligations. For organizations that so wish, compliance of the security management system with this International Standard may be verified by an external or internal auditing process.

[editorial note to the DIS:
NSBs are invited to discuss for part three of the title the desirable degree of alignment with the scope agreed to by TMB and TC 292 in the justification study - part three of the title would read:
»Requirements including aspects relevant for the supply chain«]

DRAFT INTERNATIONAL STANDARD **ISO/DIS 28000:2021(E)**

Security and resilience - Security management systems – Requirements for the supply chain

1 Scope

This International Standard 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 an 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 and 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*

ISO 31000, *Risk management — Guidelines*

3 Terms and definitions

For the purposes of this document, the terms and definitions in ISO 22300 and the following terms and definitions 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 http://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* (3.8)

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.

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
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 and interested parties 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.

3.4
management system
set of interrelated or interacting elements of an *organization* (3.1) to establish *policies* (3.7) and *objectives* (3.8) and *processes* (3.12) to achieve those objectives

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

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

Note 3 to entry: The scope of a management system can include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.

3.5
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.

3.6
effectiveness
extent to which planned activities are realized and planned results achieved

3.7
policy
intentions and direction of an *organization* (3.1), as formally expressed by its *top management* (3.5)

3.8
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 financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and *process* (3.12)).

Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, 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, security objectives are set by the organization, consistent with the security policy, to achieve specific results.

3.9
risk
effect of uncertainty on objectives

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.

3.10
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* (3.12);

— information created in order for the *organization* (3.1) to operate (documentation);

— evidence of results achieved (records).

[SOURCE: ISO/IEC 27000, 3.19]

3.12
process
set of interrelated or interacting activities which transforms inputs into outputs

3.13
performance
measurable results

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

Note 2 to entry: Performance can relate to managing activities, *processes* (3.12), products (including services), systems or *organizations* (3.1).

3.14
outsource (verb)
make an arrangement where an external *organization* (3.1) performs part of an organization’s function or *process* (3.12)

Note 1 to entry: An external organization is outside the scope of the *management system* (3.4), although the outsourced function or process is within the scope.

3.15
monitoring
determining the status of a system, a *process* (3.12) or an activity

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

3.16
measurement
process (3.12) to determine a value

3.17
audit
systematic, independent and documented *process* (3.12) for obtaining audit 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).