DRAFT INTERNATIONAL STANDARD

ISO/DIS 34001.4

ISO/TC **292**

Secretariat: **SIS**

Voting begins on:
2016-09-09

Voting terminates on:
2016-11-03

Security and resilience — Security management system for organizations assuring authenticity, integrity and trust for products and documents

Système de management de la sécurité

ICS: 03.100.01

This document is circulated as received from the committee secretariat.

Reference number
ISO/DIS 34001.4:2016(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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 on 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 the following URL: www.iso.org/iso/foreword.html.

The committee responsible for this document is Technical Committee ISO/TC 292, *Security and resilience*.

Introduction

Organizations of all types and sizes have an interest in minimizing risks to their tangible and intangible assets related to the authenticity and integrity of products and documents by protecting them from an array of harmful threats. Sources of risk that can prevent an organization from achieving its objectives can include intended or unintended acts of individuals, independently or in association with others. Protecting the tangible and intangible assets of an organization is central to security management and includes managing the consequences of security breaches. Security management includes the treatment of multiple common risks, including threats to the supply chain, proprietary and sensitive information, and physical asset protection. The organization needs to be aware of the consequences of threats in order to manage, preferably through preventative measures, consequential damage to the organization and its stakeholders. Security risks and their associated threats are unique to the organization because of geographical location, jurisdiction, sector, the nature of the product, service or end use, as well as the value to potential adversaries. The security risk profile, derived from the risk assessment of the specific threat scenarios and the existing level of protection against those threats, is unique to an organization and requires a tailor-made approach to managing its security risks. Effective management of the security risk profile requires the use of security management expertise, management activities, processes, policies, procedures, infrastructure, systems and culture.

This document specifies requirements for the performance of security management functions and processes that together enable an organization to plan, operate, maintain and improve a comprehensive security management system. Organizations can use this document to establish and implement a strategy appropriate to their security risk profile, operational and business requirements.

Organizations or relying parties can use this document to specify requirements to anticipate, identify, assess and treat security risks. This document can be used to demonstrate to internal and external stakeholders that the organization has taken appropriate measures to manage its security risks.

It is important to recognize the relationship between security, safety and quality in this document. However, security, safety and quality management need to be aligned with the organization's overall risk and business management strategy.

— A quality management system aims to define and implement the day-to-day processes necessary to consistently produce a product to specification. It focuses on normal operations with stakeholders working towards a common interest.

— A safety management system relates to the attributes of a safe product for consumption or use, or of a safe workplace. It defines those practices and processes that will render a product safe for consumption or use, or a work place safe for people and their health.

— A security management system provides a framework for an organization to manage the security risks of intentional and unintentional acts to support the delivery of quality and safe products and services. Security management focuses on assessment of security risks and treatment of those threats to the organization's activities, functions, products and services that can result in undesirable events with negative consequences to its tangible and intangible assets.

This document addresses security risks associated with individuals and organizations seeking to disrupt normal operations or to derive unauthorized benefit through harmful acts. It provides a framework for the organization to protect itself from security-related threats, in order to support normal operations, and is intended to be compatible with other ISO standards related to security.

This document can be integrated with the overall business management system within an organization. A suitably designed management system can satisfy the requirements of quality, environmental, safety, information security and supply chain standards. Organizations that have adopted an ISO approach to management systems (e.g. according to ISO 9001, ISO 14001, ISO/IEC 27001 or ISO 28000) might be able to use their existing management system as a foundation for the security management system as described in this document.

Managing security-related risks is essential in assuring the quality and safety of an organization's products and services. This document enables an organization to establish the necessary risk treatment to protect against internal and external sources of security threats. In order to establish a robust strategy, the organization needs to establish, implement and maintain a management system that addresses issues related to managing risks identified in its risk assessment, in order to minimize the likelihood and consequences of intentional and unintentional events that can cause harm to the organization and its assets, both tangible and intangible.

This document is applicable to all sizes and types of organizations in the private, not-for-profit and public sectors. The adoption of a security management system is generally a strategic decision of an organization. The design and implementation of an organization's security management system is influenced by:

a) the internal and external context in which it operates;

b) its varying needs and that of its stakeholders;

c) its objectives;

d) the products and services it provides;

e) the sensitivity of its assets and information;

f) its processes and industry sector;

g) its size and organizational structure;

h) applicable legal requirements.

The management system approach encourages organizations to analyse organizational and stakeholder requirements and define processes that contribute to a robust security strategy. A management system can provide the framework for continual improvement to increase the likelihood of enhancing security and the integrity of assets. It provides confidence to the organization and its stakeholders that the organization is able to provide a secure environment which fulfils organizational and stakeholder requirements.

The approach for security management presented in this document encourages its users to emphasise the importance of:

a) understanding an organization's risk and threat assessment, security level and asset protection requirements;

b) establishing a policy and objectives to manage the security-related risks;

c) implementing and operating controls to manage an organization's security-related risks within the context of the organization's mission;

d) monitoring and reviewing the performance and effectiveness of the security management system;

e) continual improvement based on the internal management system audit and management review.

This document adopts the Plan-Do-Check-Act (PDCA) model, which is applied to structure the security management system processes as described below.

— Plan (establish the management system): Establish management system policy, objectives, processes and procedures relevant to managing risk and improving the security management system and to delivering results in accordance with an organization's overall policies and objectives.

— Do (implement and operate the management system): Implement and operate the management system policy, controls, processes and procedures.

— Check (monitor and review the management system): Assess and measure process performance against management system policy objectives and practical experience and report the results to management for review.

— Act (maintain and improve the management system): Take corrective and preventive actions, based on the results of the internal management system audit and management review, to achieve continual improvement of the management system.

This document is applicable to an organization that wishes to:

a) develop, implement, maintain and improve a security management system;

b) give assurance of its conformity with its stated security policy;

c) demonstrate conformity with this document by:

   1) making a self-determination and self-declaration;

   2) seeking confirmation of its conformity by parties having an interest in the organization (such as customers);

   3) seeking confirmation of its self-declaration by a party external to the organization;

   4) seeking certification/registration of its security management system by an external organization.

Conformity with this document can be verified by an auditing process that is compatible and consistent with the methodology of ISO 9001, ISO 14001 and ISO/IEC 27001.

Security and resilience — Security management system for organizations assuring authenticity, integrity and trust for products and documents

1 Scope

This document addresses the management of security-related risks to an organization's tangible assets (human, financial and physical) and intangible assets (information, brand and reputation). It is intended to help an organization assure authenticity, integrity and trust for its products and documents. It addresses risks that can compromise this objective and result in events causing harm to the organization and its stakeholders. These risks include:

a) fraudulent acts;

b) deliberate acts of an adversary or competitor;

c) acts of malicious intent;

d) wilful neglect;

e) unintentional acts impacting assets.

This document specifies requirements for an organization to assess its specific security risks and address risks pertinent to its risk tolerance, in a way that is proactive in preventing acts detrimental to the organization. The security management system described in this document is intended to be an integral part of the organization's overall management system.

The requirements specified in this document are generic and intended to be applicable to all organizations (or parts thereof), regardless of the type, size and nature of the organization. The extent of application of these requirements depends on the organization's operating environment, product and service portfolio, risk profile and complexity.

This document specifies requirements for a security management system to enable an organization to establish and implement policies, objectives and programmes. This document applies to security-related risks and impacts of security-related acts that the organization needs to control, influence or reduce. It does not state specific performance criteria.

This document addresses the relevance of risks related to information technology (IT) security but is not intended to give requirements on how to manage IT security, which is addressed in ISO/IEC 27001.

This document is intended to prevent or mitigate harmful attacks on products and documents by human action that is directly contrary to the intentions of the organization producing the product or document.

2 Normative references

There are no normative references in this document.

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 http://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
stakeholder
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* (3.1) and interested parties that the need or expectation under consideration is implied.

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

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 may 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* (3.24) 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* (3.26), security objectives are set by the *organization* (3.1), consistent with the *security policy* (3.27), to achieve specific results.

3.9
risk
effect of uncertainty on *objectives* (3.8)

Note 1 to entry: An effect is a deviation from the expected — positive or negative.

Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

Note 3 to entry: Risk is often characterized by reference to potential "events" (as defined in ISO Guide 73:2009, 3.5.1.3) and "consequences" (as defined in ISO Guide 73:2009, 3.6.1.3), or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated "likelihood" (as defined in ISO Guide 73:2009, 3.6.1.1) of occurrence.

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 to operate (documentation);

— evidence of results achieved (records).

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

3.13
performance
measurable result

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

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