FINAL
DRAFT

INTERNATIONAL
STANDARD

ISO/IEC
FDIS
27014

ISO/IEC JTC **1**/SC **27**

Secretariat: DIN

Voting begins on:
2020-09-02

Voting terminates on:
2020-10-28

Information security, cybersecurity and privacy protection — Governance of information security

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.

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.

Reference number
ISO/IEC FDIS 27014:2020(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 Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection,* in collaboration with ITU-T.

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.

This second edition cancels and replaces the first edition (ISO/IEC 27014:2013), which has been technically revised. The main changes compared to the previous edition are as follows:

- the document has been aligned with ISO/IEC 27001:2013;
- the requirements in ISO/IEC 27001 which are governance activities have been explained;
- the objectives and processes of information security governance have been described.

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

Information security is a key issue for organizations, amplified by rapid advances in attack methodologies and technologies, and corresponding increased regulatory pressures.

The failure of an organization’s information security controls can have many adverse impacts on an organization and its interested parties including, but not limited to, the undermining of trust.

Governance of information security is the use of resources to ensure effective implementation of information security, and provides assurance that:

— directives concerning information security will be followed; and

— the governing body will receive reliable and relevant reporting about information security–related activities.

This assists the governing body to make decisions concerning the strategic objectives for the organization by providing information about information security that can affect these objectives. It also ensures that information security strategy aligns with the overall objectives of the entity.

Managers and others working in organizations need to understand:

— the governance requirements that affect their work; and

— how to meet governance requirements that require them to take action.

Information security, cybersecurity and privacy protection — Governance of information security

1 Scope

This document provides guidance on concepts, objectives and processes for the governance of information security, by which organizations can evaluate, direct, monitor and communicate the information security-related processes within the organization.

The intended audience for this document is:

— governing body and top management;

— those who are responsible for evaluating, directing and monitoring an information security management system (ISMS) based on ISO/IEC 27001;

— those responsible for information security management that takes place outside the scope of an ISMS based on ISO/IEC 27001, but within the scope of governance.

This document is applicable to all types and sizes of organizations.

All references to an ISMS in this document apply to an ISMS based on ISO/IEC 27001.

This document focuses on the three types of ISMS organizations given in Annex B. However, this document can also be used by other types of organizations.

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/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 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 http://www.electropedia.org/

3.1
entity
organization and other bodies or parties

Note 1 to entry: An entity can be a group of companies, or a single company, or a non for profit company, or other. The entity has governance authority over the organization. The entity can be identical to the organization, for example in smaller companies.

3.2
organization
part of an *entity* (3.1) which runs and manages an ISMS

3.3
governing body
person or group of people who are accountable for the performance and conformance of the entity

[SOURCE: ISO/IEC 27000:2018, 3.24, modified — “organization” has been replaced by “entity”]

3.4
top management
person or group of people who directs and controls an organization 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 covers only part of an organization, then top management refers to those who direct and control that part of the organization. In this situation, top management are accountable to the governing body of the entity.

Note 3 to entry: Depending on the size and resources of the organization, top management can be the same as the governing body.

Note 4 to entry: Top management reports to the governing body.

Note 5 to entry: ISO/IEC 37001 also provides definitions for governing body and top management.

[SOURCE: ISO/IEC 27000:2018, 3.75, modified — In Note 2 to entry, the second sentence has been added. Note 3 to entry has been replaced. Notes 4 and 5 to entry have been added.]

4 Abbreviated terms

EDM	evaluate, direct, monitor
ISMS	information security management system
IT	information technology

5 Use and structure of this document

This document describes how information security governance operates within an ISMS based on ISO/IEC 27001, and how these activities can relate to other governance activities which operate outside the scope of an ISMS. It outlines four main processes of “evaluate”, “direct”, “monitor” and “communicate” in which an ISMS can be structured inside an organization, and suggests approaches for integrating information security governance into organizational governance activities in each of these processes. Finally, Annex A describes the relationships between organizational governance, governance of information technology and governance of information security.

The ISMS covers the whole of the organization, by definition (see ISO/IEC 27000). It can cover the whole entity or part of it. This is illustrated in Figure B.1.

6 Governance and management standards

6.1 Overview

Governance of information security is the means by which an organization’s governing body provides overall direction and control of activities that affect the security of an organization’s information. This direction and control focuses on circumstances where inadequate information security can adversely affect the organization’s ability to achieve its overall objectives. It is common for a governing body to realise its governance objectives by:

- providing direction by setting strategies and policies;
- monitoring the performance of the organization; and
- evaluating proposals and plans developed by managers.

Management of information security is associated with ensuring the achievement of the objectives of the organization described within the strategies and policies established by the governing body. This can include interacting with the governing body by:

- providing proposals and plans for consideration by the governing body; and
- providing information to the governing body concerning the performance of the organization.

Effective governance of information security requires both members of the governing body and managers to fulfil their respective roles in a consistent way.

6.2 Governance activities within the scope of an ISMS

ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of an organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.

ISO/IEC 27001 does not use the term “governance” but specifies a number of requirements which are governance activities. The following list provides examples of these activities. References to the organization and top management are, as previously noted, associated with the scope of an ISMS based on ISO/IEC 27001.

- ISO/IEC 27001:2013, 4.1, requires the organization to identify what it is aiming to achieve – its information security goals and objectives. These should be related to, and support, the overall goals and objectives of the entity. This relates to governance objectives 1, 3 and 4 stated in 7.2.
- ISO/IEC 27001:2013, 4.2, requires the organization to identify the interested parties that are relevant to its ISMS, and the requirements of those interested parties relevant to information security. This relates to governance objective 4 stated in 7.2.
- ISO/IEC 27001:2013, 4.3, requires the organization to define the boundaries and applicability of the ISMS to establish its scope by considering the external issues and internal issues, the requirements, and interfaces and dependencies. It is also specified that "the organization shall build the requirements and expectations of interested parties into its information security management system, as well as external and internal issues (such as laws, regulations and contracts)". This relates to governance objective 1 stated in 7.2.
- ISO/IEC 27001:2013, Clause 5, specifies that "the organization shall set policy, objectives and integrate information security into its processes (which can be considered to include governance processes)". It requires the organization to make suitable resources available and communicate the importance of information security management. Most importantly, it also states that "the organization shall direct and support persons to contribute to the effectiveness of the ISMS, and that other relevant management roles shall be supported in their areas of responsibility". ISO/IEC 27001:2013, Clause 5, contains instructions for setting policy, and assigning roles for information security management and reporting. This relates to governance objectives 1 and 3 stated in 7.2.
- ISO/IEC 27001:2013, Clause 6, considers the design of a risk management approach for the organization, specifying that "the organization shall identify risks and opportunities to be addressed to ensure that its ISMS is effective". It introduces the concept of risk owners, and puts their responsibilities into the context of the organization’s activities to manage risk and approve risk

treatment activities. It also requires the organization to establish information security objectives. This relates to governance objective 2 stated in 7.2.

- ISO/IEC 27001:2013, Clause 7, specifies that "persons shall be competent in carrying out their information security obligations". It also provides a requirement for organizational communications. This relates to governance objective 5 stated in 7.2.
- ISO/IEC 27001:2013, Clause 8, requires the organization to plan, implement and control its ISMS, including outsourced arrangements. This relates to governance objectives 4 and 6 stated in 7.2.
- ISO/IEC 27001:2013, Clause 9, requires monitoring and reporting of all relevant aspects of the ISMS, internal audits, and top management and governing body review and decisions on the operational effectiveness of the ISMS, including any changes required. This relates to governance objective 6 stated in 7.2.
- ISO/IEC 27001:2013, Clause 10, specifies the identification and treatment of non-conformities, the requirement for identification of opportunities for continual improvement and acting on those opportunities. This relates to governance objective 4 stated in 7.2.

6.3 Other related standards

ISO/IEC 38500 provides guiding principles for members of governing bodies of organizations on the effective, efficient and acceptable use of information technology within their organizations. It also provides guidance to those advising, informing or assisting governing bodies in governance of IT.

6.4 Thread of governance within the organization

These threads are in exact correspondence to the organizational governance processes described in Clause 7. The last two items in the list are equivalents of their governance aspects in the context of information security:

- the alignment of the information security objectives with the business objectives;
- the management of information security risk in accordance with those information security objectives;
- the avoidance of conflicts of interest in the management of information security;
- preventing the organization's information technology from being used to harm other organizations.

7 Entity governance and information security governance

7.1 Overview

There are many areas of governance within an entity, including information security, information technology, health and safety, quality and finance. Each governance area is a component of the overall governance objectives of an entity, and thus should be aligned with the discipline of the entity. The scopes of governance models sometimes overlap. 7.2 and 7.3 describe objectives and processes involved in information security governance, which can apply to any area being governed.

An ISMS focuses on management of risks relating to information. It does not directly address subjects such as profitability, acquisition, use and realization of assets, or the efficiency of other processes, although it should support any organizational objectives on these subjects.