DRAFT INTERNATIONAL STANDARD

ISO/IEC DIS 27014

ISO/IEC JTC **1**/SC **27** Secretariat: **DIN**

Voting begins on:
2020-01-10

Voting terminates on:
2020-04-03

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

ICS: 35.030

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/IEC DIS 27014:2020(E)

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

Published in Switzerland

Contents

Foreword

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating, and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a world-wide basis. The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups that, in turn, produce Recommendations on these topics. The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1. In some areas of information technology that fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

ISO (the International Organization for Standardization) and IEC (the International Electro technical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of Recommendation | International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of Information security, cybersecurity and privacy protection, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

This Recommendation | International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare this Recommendation | International Standards. Draft Recommendation | International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27014 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. The identical text is published as ITU-T Recommendation X.1054.

Summary

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 may 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.

Keyword

Information Security, Information Security Management, ISMS, Information Security Governance, EDM-model

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

1 Scope

This Recommendation | International Standard 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 ISMS (Information Security Management Systems) based upon ISO/IEC 27001
- Those responsible for information security management that takes place outside the scope of an ISMS based upon ISO/IEC 27001, but within the scope of governance.

This Recommendation | International Standard is applicable to all types and sizes of organizations.

All references to an ISMS in this document apply to an ISMS based upon 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 Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

3 Definitions

For the purposes of this Recommendation | International Standard, the terms and definitions given in ISO/IEC 27000, ISO 19011, and the following apply.

ISO, IEC and ITU-T maintain terminological databases for use in standardization at the following addresses:

- ITU-T Terms and Definitions: available at http://www.itu.int/go/terminology-database
- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

Specific definitions of relevance to this document:

3.1 entity

Noun: a thing with distinct or independent existence.

[Oxford English Dictionary]

Note 1 to entry In the context of this standard, the entity encompasses both the organization and other bodies or parties. An entity may be a group of companies, or a single company, or non for profit company, or other. The entity has governance authority over the organization. The entity may be identical to the organisation, for example in smaller companies.

3.2 organization

Noun: an organized group of people with a particular purpose, such as a business or government department.

[Oxford English Dictionary]

Note 1 to entry In the context of this standard, an organization is that which implements the ISMS.

3.3 governing body

Person or group of people who are accountable for the performance and conformance of the entity [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 entity, then top management refers to those who direct and control that part of the entity. In this situation, top management are accountable to the governing body of the entity.

Note 3 to entry Depending on the size andresources of the organization, top management may be the same as the governing body.

Note 4 to entry Top management reports to the governing body. [ISO/IEC 27000:2018, 3.75].

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

4 Abbreviations

EDM	Evaluate, Direct, Monitor
ISMS	Information Security Management System
IT	Information Technology

5 Conventions

No conventions.

6 Use and structure of this Recommendation | International Standard

This Recommendation | International Standard describes how information security governance operates within an ISMS based upon 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.

An organization is the part of an entity which runs and manages an ISMS. The ISMS covers the whole of the organization, by definition (see ISO/IEC 27000); it may not cover the whole of the entity. This is illustrated in Figure B.1.

7 Governance and management standards

7.1 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.

7.2 Governance activities within the scope of an ISMS

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. In the subclauses, references to the organization and top management are, as previously noted, associated with the scope of an ISMS based on ISO/IEC 27001.

- Subclause 4.1, Understanding the organization and its context, 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 8.2 of this document.
- Subclause 4.2, Understanding the needs and expectations of interested parties, 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 8.2 of this document.
- Subclause 4.3, Determining the scope of the ISMS, 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 8.2 of this document.

- Clause 5, Leadership, specifies that the organization shall set policy, objectives, and integrate information security into its processes (which may 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. The clause contains instructions for setting policy, and assigning roles for information security management and reporting. This relates to governance objectives 1 and 3 stated in 8.2 of this document.

- Clause 6, Planning, 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 will be 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 8.2 of this document.

- Clause 7, Support, specifies that persons shall be competent in carrying out their information security obligations, and provides a requirement for organizational communications. This relates to governance objective 5 stated in 8.2 of this document.

- Clause 8, Operation, specifies the responsibility of the organization to plan, implement and control its ISMS, including outsourced arrangements.

- Clause 9, Performance evaluation, 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 8.2 of this document.

- Clause 10, Improvement, 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 8.2 of this document.

7.3 The role of ISO/IEC 27001

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.

7.4 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.

7.5 Thread of governance within the organization

These threads are in exact correspondence to the organizational governance processes described in Clause 8. 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.