INTERNATIONAL STANDARD

ISO/IEC 27014

Second edition
2020-12

Corrected version
2022-04

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

Sécurité de l'information, cybersécurité et protection de la vie privée — Gouvernance de la sécurité de l'information

Reference number
ISO/IEC 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

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of 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.

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 document should be noted (see www.iso.org/directives or www.iec.ch/members_experts/refdocs)

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. 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) or the IEC list of patent declarations received (see https://patents.iec.ch).

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. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by ITU-T as ITU-T X.1054 (04/2021) and drafted in accordance with its editorial rules, in collaboration with Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection.*

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.

This corrected version of ISO/IEC 27014:2020 incorporates the following corrections:

- the document has been editorially revised in accordance with the rules-for-presentation-ITU-T-ISO-IEC common text.

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 and www.iec.ch/national-committees.

INTERNATIONAL STANDARD ISO/IEC 27014
RECOMMENDATION ITU-T X.1054

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

Summary

Recommendation ITU-T X.1054 | International Standard ISO/IEC 27014 provides guidance on the governance of information security.

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.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1054	2012-09-07	17	11.1002/1000/11594
2.0	ITU-T X.1054	2021-04-30	17	11.1002/1000/14248

Keywords

Information security, information security governance, information security management, ISMS.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). 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 worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, 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 which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Introduction

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 Standard has been 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 Standard. 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 Recommendation | International Standard may be the subject of patent rights. ITU, ISO or IEC shall not be held responsible for identifying any or all such patent rights.

Rec. ITU-T X.1054 | 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 SG17.

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

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 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 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 on ISO/IEC 27001.

This Recommendation | International Standard focuses on the three types of ISMS organizations given in Annex B. However, it 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 27000:in force, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.
- – ISO/IEC 27001:in force, *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, and the following apply.

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

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

3.1 **entity**: Organization (3.2) and other bodies or parties.

NOTE – 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**: That 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.

NOTE – 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 (3.2) at the highest level.

NOTE 1 – Source ISO/IEC 9001.

NOTE 2 – Top management has the power to delegate authority and provide resources within the organization.

NOTE 3 – 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 4 – Depending on the size and resources of the organization, top management can be the same as the governing body.

NOTE 5 – Top management reports to the governing body. [SOURCE: ISO/IEC 27000:2018, 3.75].

NOTE 6 – ISO/IEC 37001 also provides definitions for governing body and top management.

4 Abbreviations

For the purposes of this Recommendation | International Standard, the following abbreviations apply:

ISMS	Information Security Management System
IT	Information Technology

5 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.

The ISMS covers the whole of the organization, by definition (see ISO/IEC 27000). It can cover the whole of the entity, or part of the entity. 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 of this Recommendation | International Standard.
- 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 of this Recommendation | International Standard.
- 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 of this Recommendation | International Standard.
- ISO/IEC 27001:2013, 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, 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 of this Recommendation | International Standard.
- ISO/IEC 27001:2013, 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 of this Recommendation | International Standard.
- ISO/IEC 27001:2013, 7 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 7.2 of this Recommendation | International Standard.
- ISO/IEC 27001:2013, 8 specifies the responsibility of the organization to plan, implement and control its ISMS, including outsourced arrangements. This relates to governance objectives 4 and 6 stated in 7.2 of this Recommendation | International Standard.
- ISO/IEC 27001:2013, 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 of this Recommendation | International Standard.
- ISO/IEC 27001:2013, 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 of this Recommendation | International Standard.

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 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.