INTERNATIONAL ISO/IEC

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.

 

# 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/.