INTERNATIONAL STANDARD

ISO/IEC 27014

Second edition
2020-12

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)

COPYRIGHT PROTECTED DOCUMENT

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*