
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*



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2020

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	2
5 Use and structure of this document	2
6 Governance and management standards	2
6.1 Overview	2
6.2 Governance activities within the scope of an ISMS	3
6.3 Other related standards	4
6.4 Thread of governance within the organization	4
7 Entity governance and information security governance	4
7.1 Overview	4
7.2 Objectives	5
7.2.1 Objective 1: Establish integrated comprehensive entity-wide information security	5
7.2.2 Objective 2: Make decisions using a risk-based approach	5
7.2.3 Objective 3: Set the direction of acquisition	5
7.2.4 Objective 4: Ensure conformance with internal and external requirements	5
7.2.5 Objective 5: Foster a security-positive culture	6
7.2.6 Objective 6: Ensure the security performance meets current and future requirements of the entity	6
7.3 Processes	6
7.3.1 General	6
7.3.2 Evaluate	7
7.3.3 Direct	8
7.3.4 Monitor	8
7.3.5 Communicate	9
8 The governing body's requirements on the ISMS	9
8.1 Organization and ISMS	9
8.2 Scenarios (see Annex B)	10
Annex A (informative) Governance relationship	12
Annex B (informative) Types of ISMS organization	13
Annex C (informative) Examples of communication	15
Bibliography	16

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.