

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)

© ISO/IEC 2020



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