
**Information technology — Security
techniques — Governance of information
security**

*Technologies de l'information — Techniques de sécurité —
Gouvernance de la sécurité de l'information*



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2013

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

CONTENTS

Page

Summary	iv
Foreword	v
1 Scope.....	1
2 Normative references	1
3 Definitions	1
4 Concepts	2
4.1 General.....	2
4.2 Objectives.....	2
4.3 Desired Outcomes.....	2
4.4 Relationship	2
5 Principles and processes.....	3
5.1 Overview	3
5.2 Principles.....	3
5.3 Processes.....	5
5.3.1 Overview	5
5.3.2 Evaluate.....	5
5.3.3 Direct	6
5.3.4 Monitor.....	6
5.3.5 Communicate.....	6
5.3.6 Assure.....	7
Annex A (informative) An example of information security status	8
Annex B (informative) An example of detailed information security status.....	9
Bibliography.....	11

INTERNATIONAL STANDARD <ISO/IEC 27014>

ITU-T RECOMMENDATION <X.1054>

**Information technology — Security techniques —
Governance of information security**

Summary

This Recommendation | International Standard provides guidance on the governance of information security.

Information security has become a key issue for organisations. Not only are there increasing regulatory requirements but also the failure of an organisation's information security measures can have a direct impact on an organisation's reputation.

Therefore, the governing body, as part of its governance responsibilities, is increasingly required to oversee information security to ensure the objectives of the organisation are achieved.

In addition, governance of information security provides a powerful link between an organisation's governing body, executive management and those responsible for implementing and operating an information security management system.

It provides the mandate essential for driving information security initiatives throughout the organisation.

Furthermore, an effective governance of information security ensures that the governing body receives relevant reporting - framed in a business context - about information security-related activities. This enables pertinent and timely decisions about information security issues in support of the strategic objectives of the organisation.