INTERNATIONAL STANDARD

ISO/IEC 27014

First edition
2013-05-15

Information technology — Security techniques — Governance of information security

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

Reference number
ISO/IEC 27014:2013(E)

COPYRIGHT PROTECTED DOCUMENT

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

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.

Foreword

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. 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 world-wide basis. The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups that, 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 that fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

ISO (the International Organisation for Standardization) and IEC (the International Electro technical 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 organisation to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organisations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 27014 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*, in collaboration with ITU-T. The identical text is published as ITU-T Recommendation X.1054.

1 Scope

This Recommendation | International Standard provides guidance on concepts and principles for the governance of information security, by which organisations can evaluate, direct, monitor and communicate the information security related activities within the organisation.

This International Standard is applicable to all types and sizes of organisations.

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

ISO/IEC 27000:2009, *Information Technology – Security techniques – Information security management systems – Overview and vocabulary*

3 Definitions

For the purposes of this Recommendation | International Standard, the terms and definitions in ISO/IEC 27000:2009 and the following definitions apply:

3.1
executive management
person or group of people who have delegated responsibility from the governing body for implementation of strategies and policies to accomplish the purpose of the organisation.

NOTE 1 Executive management form part of top management: For clarity of roles, this standard distinguishes between two groups within top management: the governing body and executive management.

NOTE 2 Executive management can include Chief Executive Officers (CEOs), Heads of Government Organizations, Chief Financial Officers (CFOs), Chief Operating Officers (COOs), Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), and like roles.

3.2
governing body
person or group of people who are accountable for the performance and conformance of the organisation

NOTE Governing body forms part of top management: For clarity of roles, this standard distinguishes between two groups within top management: the governing body and executive management.

3.3
governance of information security
system by which an organisation's information security activities are directed and controlled

3.4
stakeholder
any person or organisation that can affect, be affected by, or perceive themselves to be affected by an activity of the organisation.

NOTE A decision maker can be a stakeholder.