



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1054

(09/2012)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Information and network security – Security management

Information technology - Security techniques - Governance of information security

CAUTION !

PREPUBLISHED RECOMMENDATION

This prepublication is an unedited version of a recently approved Recommendation. It will be replaced by the published version after editing. Therefore, there will be differences between this prepublication and the published version.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). 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 worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, 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 which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU [had/had not] received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2012

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Recommendation ITU-T X.1054 | ISO/IEC 27014, Information technology - Security techniques - Governance of information security

Contents

1 Scope 2

2 Normative references 2

3 Definitions 2

4 Concepts 3

 4.1 General 3

 4.2 Objectives 3

 4.3 Desired Outcomes 3

 4.4 Relationship 3

5 Principles and processes 4

 5.1 Overview 4

 5.2 Principles 4

 5.3 Processes 6

 5.3.1 Overview 6

 5.3.3 Direct 6

 5.3.4 Monitor 7

 5.3.5 Communicate 7

 5.3.6 Assure 7

Annex A An example of information security status 9

Annex B An example of detailed information security status 10

Bibliography 11

Recommendation ITU-T X.1054 | ISO/IEC 27014, 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.

1 Scope

This Recommendation | International Standard provides concepts and guidance on principles and processes for the governance of information security, by which organisations can evaluate, direct and monitor the management of information security.

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 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 is from part of top management: For clarity of roles, this standard distinguishes between two groups within top management: the governing body and executive managers.

NOTE 2 – Executive management can include Chief Executive Officers, Chief Financial Officers, (CFOs), Chief Operating Officers (COOs), Chief Information Officers, (CIOs), Chief Information Security Officers (CISOs), and like roles.