

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1052

(05/2011)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Information and network security – Security management

Information security management framework

Recommendation ITU-T X.1052

ITU-T X-SERIES RECOMMENDATIONS
DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1052

Information security management framework

Summary

Recommendation ITU-T X.1052 describes and recommends the framework of information security management for telecommunications to support Recommendation ITU-T X.1051 and other Recommendations in the ITU-T X.105x-series. The information security management framework (ISMF) is based on a process approach to describe a set of security management areas which gives guidelines to telecommunications to fulfil the control object defined in Recommendation ITU-T X.1051 and other Recommendations in the ITU-T X.105x-series. The management areas, which include asset management, incident management, risk management and policy management, map the controls defined by Recommendation ITU-T X.1051 to the implementation methodologies. This way ISMF relates Recommendation ITU-T X.1051, which provides management guidelines for telecommunication organizations, to other Recommendations, such as Recommendations ITU-T X.1055 and ITU-T X.1056, which provide practical methodologies focusing on a specific area of information security management.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1052	2011-05-29	17

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 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.

Table of Contents

	Page
1 Scope	1
2 References.....	1
3 Definitions	1
3.1 Terms defined elsewhere	1
3.2 Terms defined in this Recommendation.....	1
4 Abbreviations.....	1
5 Conventions	2
6 Information security management framework in telecommunication organizations ...	2
6.1 Objective.....	2
6.2 Overview of the information security management framework.....	2
7 Policy management.....	4
7.1 Overview	4
7.2 Main activities	5
8 Risk management	5
8.1 Overview	5
8.2 Main activities	6
9 Organization and personnel	7
9.1 Overview	7
9.2 Main activities	8
10 Asset management.....	9
10.1 Overview	9
10.2 Main activities	9
11 System acquisition and development.....	10
11.1 Overview	10
11.2 Main activities	10
12 Operations and maintenance management	12
12.1 Overview	12
12.2 Main activities	12
13 Incident management.....	17
13.1 Overview	17
13.2 Main activities	18
Bibliography.....	19

Recommendation ITU-T X.1052

Information security management framework

1 Scope

This Recommendation provides the information security management framework (ISMF). ISMF maps the controls defined by [ITU-T X.1051] to the practical implementation methodologies by defining a set of management areas, such as asset management, incident management, risk management, policy management and others. This Recommendation gives an overview of the framework and analyses the relationships between these areas. The specific guidelines of each area defined in this Recommendation are provided in a series of other ITU-T Recommendations.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

- [ITU-T X.1051] Recommendation ITU-T X.1051 (2008) | ISO/IEC 27011:2008, *Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*.
- [ITU-T X.1055] Recommendation ITU-T X.1055 (2008), *Risk management and risk profile guidelines for telecommunication organizations*.
- [ITU-T X.1056] Recommendation ITU-T X.1056 (2009), *Security incident management guidelines for telecommunication organizations*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

None.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 configuration item: A security configuration item is a specific security configuration requirement of a specific class of assets, which includes the description of the requirement, the reference method for the implementation of the requirement, and the conditions to check whether the requirement be complied or not.

3.2.2 configuration profile: A group of configuration items suitable for a special class of asset.

4 Abbreviations

This Recommendation uses the following abbreviations and acronyms:

ISIRT Information Security Incident Response Team

ISMF Information Security Management Framework
 ISMS Information Security Management System
 IT Information Technology

5 Conventions

None.

6 Information security management framework in telecommunication organizations

6.1 Objective

[ITU-T X.1051] defines categories of security controls for telecommunication organization security management, such as security policy, organization of information security, and human resources security, among others. ISMF defines a series of main activities to conduct and support the implementation of security controls. ISMF combines the controls in [ITU-T X.1051] and the Recommendations which define implementation methodologies for a number of management areas, such as [ITU-T X.1055] and [ITU-T X.1056].

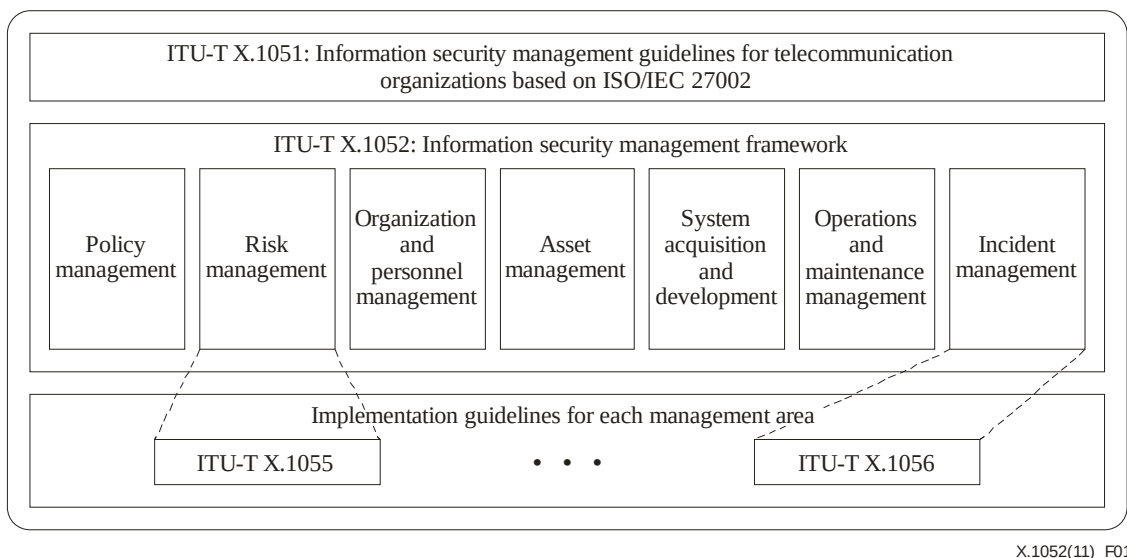


Figure 1 – Relationship between Recommendation ITU-T X.1052 and other ITU-T X.105x-series Recommendations

6.2 Overview of the information security management framework

It is necessary for telecommunication organizations to confirm the scope of their information security management system (ISMS), which includes information assets. The guidelines for implementing the information security management and this confirmation should be carried out before assessing the risks to their information assets and determining the subsequent controls of the risks. In addition, it is necessary to establish the structure and form of the information security organization as the base for the implementation of information security for controlling the risks. The risk-controlling activities of the telecommunication organizations should not be isolated from the operations of the organizations. The operations of the organization are generally described in a series of procedures. The risk-controlling activities of information security should be regarded as an integral part of the relevant procedures.

The ISMF describes the main activities related to telecommunication organizations and information security management from the three aspects:

- a) supporting the implementation of information security management within telecommunication organizations, including management areas such as organization and personnel management and asset management;
- b) establishing and continually improving the ISMS, including management areas such as risk management and policy management;
- c) specific operational activities of the telecommunication organization, including management areas such as system acquisition and development management, operation and maintenance management, and incident management.

The seven management areas shown in Figure 1 are, on one hand, a summary of the management activities of a telecommunication organization which are strongly related with the operation of the organization. These, on the other hand, correspond closely to the controls specified in [ITU-T X.1051]. Activities that relate to the organization and personnel management serve and comply with the control objectives defined in the clauses "Organization of information security" and "Human resources security" of [ITU-T X.1051]. In the same way, asset management mainly serves the control objectives described in the "Asset management" and "Physical and environmental security" of [ITU-T X.1051]. Risk management primarily serves to support the control objectives described in the "Communications and operations management", "Access control" and "Information systems acquisition, development and maintenance" of [ITU-T X.1051]. Finally, incident management primarily supports the control objectives given in the "Information security incident management" and "Business continuity management" of [ITU-T X.1051].

The security policy of an organization defines the aims of information security management of the organization, clarifies the management requirements of information security, and provides the necessary suggestions or guidelines. The aim and scope of information security, the purpose of the management, control objects selected and the framework of controlling measures can also be found in the policy.

Risk management should involve the following activities: analyse the threats the organization faces, examine the vulnerabilities of the organization's assets, implement the controls to mitigate the organization's risks and continually improve the effectiveness of the organization information security.

Asset management is an essential aspect of the scope of the ISMS of the telecommunication organization. Asset management involves identifying the assets of the organization, defining the rules for classifying and valuing assets, managing asset inventories, confirming the ownership of assets and reviewing and monitoring asset changes.

By establishing a security organization and confirming the duties of the personnel, organization and personnel management is likely to guarantee the execution of other management activities in the ISMF, such as security policy management and risk management. The main activities of organization and personnel management include clarifying the commitment of the management, founding the relevant responsibility framework and controlling measures, screening the candidates prior to employment, providing the security-relevant education and training during employment, defining and assigning responsibilities for performing employment termination.