

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X

Supplement 13

(09/2012)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

ITU-T X.1051 – Supplement on information security management users' guide for Recommendation ITU-T X.1051

ITU-T X-series Recommendations – Supplement 13

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.

Supplement 13 to ITU-T X-series Recommendations

ITU-T X.1051 – Supplement on information security management users' guide for Recommendation ITU-T X.1051

Summary

Supplement 13 to ITU-T X-series Recommendations provides interpretable guidance for users of Recommendation ITU-T X.1051. This Supplement gives additional explanations and further implementation guidance for each clause and control specified in Recommendation ITU-T X.1051.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X Suppl. 13	2012-09-07	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 publication, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the publication 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 publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication 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 publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. 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 2013

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 and abbreviations	1
	3.1 Definitions	1
	3.2 Abbreviations	1
4	Overview	2
	4.1 Background.....	2
	4.2 Structure	2
5	Security policy	2
6	Organization of information security.....	3
	6.1 Internal organization.....	3
	6.2 External parties	4
7	Asset management	5
	7.1 Responsibility for assets	5
	7.2 Information classification	5
8	Human resources security	6
	8.1 Prior to employment	6
	8.2 During employment.....	7
	8.3 Termination or change of employment	7
9	Physical and environmental security	7
	9.1 Security areas.....	7
	9.2 Equipment security	9
10	Communications and operations management	10
	10.1 Operational procedures and responsibilities.....	10
	10.2 Third party service delivery management	11
	10.3 System planning and acceptance	11
	10.4 Protection against malicious and mobile code	11
	10.5 Back-up.....	12
	10.6 Network security management	12
	10.7 Media handling.....	12
	10.8 Exchange of information	12
	10.9 Electronic commerce services	12
	10.10 Monitoring.....	12
11	Access control.....	13
	11.1 Business requirement for access control	13
	11.2 User access management	14
	11.3 User responsibilities	14



Documents

Document Sharing Hub

X series – Supplement 13 (09/2012)

iii

	Page
11.4 Network access control.....	14
11.5 Operating system access control	14
11.6 Application and information access control	14
11.7 Mobile computing and teleworking.....	14
12 Information systems acquisition, development and maintenance	14
12.1 Security requirements of information systems	14
12.2 Correct processing in applications.....	14
12.3 Cryptographic controls	14
12.4 Security of system files	14
12.5 Security in development and support processes.....	15
12.6 Technical vulnerability management	15
13 Information security incident management	15
13.1 Reporting information security events and weaknesses.....	15
13.2 Management of information security incidents and improvements	16
14 Business continuity management	17
14.1 Information security aspects of business continuity management	17
15 Compliance	18
Annex A – Telecommunications extended control set	19
A.9 Physical and environmental security	19
A.10 Communications and operations management.....	21
A.11 Access control	23
Bibliography.....	25

Supplement 13 to ITU-T X-series Recommendations

ITU-T X.1051 – Supplement on information security management users' guide for Recommendation ITU-T X.1051

1 Scope

The scope of this Supplement is to provide interpretable guidance for users of [ITU-T X.1051]. This Supplement gives additional explanations and further implementation guidance for each clause and control specified in [ITU-T X.1051]. This Supplement is intended to assist telecommunication organizations in the implementation of information security management based on [ITU-T X.1051].

2 References

- [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*.
- [ISO/IEC 27002] ISO/IEC 27002:2005, *Information technology – Security techniques – Code of practice for information security management*.
<http://webstore.iec.ch/preview/info_isoiec27002%7Bed1.0%7Den.pdf>

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this Supplement, the definitions given in [ITU-T X.1051] and [ISO/IEC 27002] apply.

3.2 Abbreviations

This Supplement uses the following abbreviations and acronyms:

ASP	Application Service Provider
DDoS	Distributed Denial of Service
DoS	Denial of Service
IDC	Internet Data Centre
IP	Internet Protocol
IPS	Intrusion Prevention System
ISP	Internet Service Provider
LAN	Local Area Network
SIP	Session Initiation Protocol
SSID	Service Set Identifier
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network

4 Overview

4.1 Background

In establishing information security management, it is essential to take account of telecommunication-specific requirements. Telecommunication organizations, the facilities of which are used by various users to process information such as personal data, confidential data and business data, should handle this information with due care and attention in order to apply an appropriate level of protection.

[ITU-T X.1051] is a guideline for telecommunication organizations to support their implementation of information security management based on [ISO/IEC 27002]. [ITU-T X.1051] has a format similar to that of [ISO/IEC 27002], and includes additional guidance and telecommunication-specific controls in addition to those contained in [ISO/IEC 27002]. Specifically, this guidance covers:

- cases where objectives and controls specified in [ISO/IEC 27002] are applicable without the need for any additional information and only a reference is provided to [ISO/IEC 27002];
- telecommunication sector-specific set of control and implementation guidance as described in Annex A; and
- cases where controls need additional guidance specific to telecommunications; here the ISO/IEC 27002 control and implementation guidance are repeated without modification, followed by the specific telecommunication guidance related to this control.

4.2 Structure

This Supplement will assist telecommunication organizations to understand the telecommunication-specific controls and the implementation guidance in [ITU-T X.1051] by providing additional detailed explanations, examples of implementation and best practices.

The structure of clauses 5 to 15 and Annex A are the same as in [ITU-T X.1051]. This Supplement specifically focuses on those clauses where additional guidance is needed:

- Organization of information security (clause 6)
- Asset management (clause 7)
- Human resources security (clause 8)
- Physical and environmental security (clause 9)
- Communications and operations management (clause 10)
- Access control (clause 11)
- Information systems acquisition, development and maintenance (clause 12)
- Information security incident management (clause 13)
- Business continuity management (clause 14)
- Telecommunications extended control set (Annex A).

5 Security policy

Telecommunication-specific implementation guidance is not included in clause 5 of [ITU-T X.1051].

6 Organization of information security

6.1 Internal organization

Objective: To manage information security within the organization.

6.1.1 Management commitment to information security

Telecommunication-specific implementation guidance is not included in clause 6.1.1 of [ITU-T X.1051].

6.1.2 Information security coordination

Telecommunication-specific implementation guidance is not included in clause 6.1.2 of [ITU-T X.1051].

6.1.3 Allocation of information security responsibilities

Telecommunication-specific implementation guidance is not included in clause 6.1.3 of [ITU-T X.1051].

6.1.4 Authorization process for information processing facilities

Telecommunication-specific implementation guidance is not included in clause 6.1.4 of [ITU-T X.1051].

6.1.5 Confidentiality agreements

(Refer to Control and Telecommunications-specific implementation guidance in clause 6.1.5 of [ITU-T X.1051].)

To protect confidential information, the non-disclosure agreement is concluded not only between the organizations (the ordering party and the accepting party) but also between the employer and employees who work in the organization. Signature is often obtained in a written oath which includes not only compliance with confidential information rules but also obligations in case of any information security incident, obligations at the time of transfer or retirement and prohibited acts.

As for the non-disclosure agreement, a template should be prepared, which accounts for differences being generated at each time the agreement is concluded. The template should include information such as content, definition of confidential information protection, the period of confidentiality, disclosure of confidential information, procedures at the time of termination of the agreement and measures in case of breach of agreement.

Since telecommunication organizations should ensure the secrecy of communications at the request of existing laws and regulations, non-disclosure agreements should be made by taking into account the protection of the communicated information. Five examples for consideration are described in clause 6.1.5 of [ITU-T X.1051]. There may be other considerations due to domestic legislation.

6.1.6 Contact with authorities

(Refer to Control and Telecommunications-specific implementation guidance in clause 6.1.6 of [ITU-T X.1051].)

The relevant parties to which the organization is required to give notice or report are specified beforehand, and the communication route (from whom to whom) is provided. Examples of the relevant parties could include police stations, fire stations, hospitals, electric companies and telecommunication organizations. Other relevant parties could be external contractors including maintenance companies and press organizations. It is desirable that the list of such addresses and telephone numbers be made available on the premises.

On the other hand, telecommunication organizations should be careful about enquiries originating from the authorities because they should ensure the secrecy of communications and the confidentiality of information of their subscribers.

6.1.7 Contact with special interest groups

Telecommunication-specific implementation guidance is not included in clause 6.1.7 of [ITU-T X.1051].

6.1.8 Independent review of information security

Telecommunication-specific implementation guidance is not included in clause 6.1.8 of [ITU-T X.1051].

6.2 External parties

Objective: To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to or managed by external parties.

6.2.1 Identification of risks related to external parties

Telecommunication-specific implementation guidance is not included in clause 6.2.1 of [ITU-T X.1051].

6.2.2 Addressing security when dealing with customers

(Refer to Control and Telecommunications-specific implementation guidance in clause 6.2.2 of [ITU-T X.1051].)

Requirements for customers concerning information security of services provided by the organization are specified and disclosed to customers after necessary measures are taken.

Requirements for customers are often stipulated in the rules for members and the rules for service use. As concrete items, appropriate use of IDs and passwords, prohibition of acts that may result in the loss of service credibility and prohibition of acts that may place an excessive burden on the system, are given.

When telecommunication organizations allow customers to access the organization's assets, it is possible that customers could, through negligence or malice, suspend the telecommunication services or degrade their quality. Telecommunication organizations should consider those concerns when making agreements with customers.

6.2.3 Addressing security in third-party agreements

(Refer to Control and Telecommunications-specific implementation guidance in clause 6.2.3 of [ITU-T X.1051].)

As for temporary staff and employees of the entrusted company who have not concluded an agreement with the organization, requirements concerning information security are described in the agreement with the company they belong to. This includes that a written oath concerning the information security observance is signed between the companies that the temporary staff belongs to or the contractor and the employee (see clause 8.1.3 of [ITU-T X.1051]).

Execution of the information security audit on a third party to whom work is consigned is described in the agreement. Moreover, timing in which the information security audit is executed is provided. Additionally, items concerning improvement of information security maintenance are described in the agreement.

When telecommunication organizations allow a third party to access the organization's assets, it is possible that the third party could, through negligence or malice, suspend telecommunication services or degrade their quality. Telecommunication organizations should consider those concerns when making agreements with third parties.

7 Asset management

7.1 Responsibility for assets

Objective: To achieve and maintain appropriate protection of organizational assets.

7.1.1 Inventory of assets

(Refer to Control and Telecommunications-specific implementation guidance in clause 7.1.1 of [ITU-T X.1051].)

Each acquisition of information assets should be listed and recorded in the information asset management inventory. The management inventory mainly describes, in addition to the standard attribute information of the information assets, items which may be reviewed with environmental changes and items needed when the information assets are disposed of.

When new information is made based on a third party's information, an agreement is obtained so as not to violate the third party's intellectual property right.

Telecommunication organizations own many specific assets compared to general organizations. Examples of the telecommunication-specific assets are classified into seven groups, as described in clause 7.1.1 of [ITU-T X.1051].

7.1.2 Ownership of assets

Telecommunication-specific implementation guidance is not included in clause 7.1.2 of [ITU-T X.1051].

7.1.3 Acceptable use of assets

Telecommunication-specific implementation guidance is not included in clause 7.1.3 of [ITU-T X.1051].

7.2 Information classification

Objective: To ensure that information receives an appropriate level of protection.

7.2.1 Classification guidelines

(Refer to Control and Telecommunications-specific implementation guidance in clause 7.2.1 of [ITU-T X.1051].)

Information is classified in terms of business impact and extent of caution in handling information. Classification guidelines should provide methods and approval procedures for classifying, transferring, retaining and disposing of information, depending on the level of sensitivity and criticality.

The sensitivity and criticality of information is often classified into three to five levels. The scope of disclosure (access rights) of information is set depending on the level of sensitivity and criticality. Moreover, the retention period of information is set in consideration of the deterioration of the sensitivity and criticality level of information as time passes.

In cases of disclosure and retrieval of information of a high degree of importance, approval is obtained from the person in charge depending on the level of sensitivity and criticality. After minimizing the number of transferring destinations, a record as to the disclosure, retrieval and return of this information is created and kept.