

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1053

(11/2017)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Information and network security – Security management

Code of practice for information security controls based on ITU-T X.1051 for small and medium-sized telecommunication organizations

Recommendation ITU-T X.1053

ITU-T

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 (1)	
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 (1)	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 (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Security protocols (2)	X.1450–X.1459
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
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

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

Recommendation ITU-T X.1053

Code of practice for information security controls based on ITU-T X.1051 for small and medium-sized telecommunication organizations

Summary

Recommendation ITU-T X.1053 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security controls in small and medium-sized telecommunication organizations (SMTOs) based on Recommendation ITU-T X.1051. This Recommendation also provides an implementation baseline of information security controls for SMTOs to ensure the confidentiality, integrity and availability of telecommunication facilities and services and information handled, processed or stored by the facilities and services.

The objectives of this Recommendation are to provide practical guidance suited for SMTOs on commonly accepted goals of information security specifically suited for these organizations.

As a result of implementing this Recommendation, SMTOs, both within and between jurisdictions, will:

- a) be able to ensure the confidentiality, integrity and availability of the specific SMTO facilities and services and the information handled, processed or stored within the facilities and services;
- b) have adopted secure collaborative processes and controls ensuring the lowering of risks in the delivery of telecommunication services;
- c) be able to deliver information security in an effective and efficient manner;
- d) have adopted a consistent holistic approach to information security; and
- e) be able to improve the security culture of organizations, raise staff awareness and increase public trust.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1053	2017-11-13	17	11.1002/1000/13367

Keywords

Availability, confidentiality, controls, integrity, security, SMTO.

* To access the Recommendation, type the URL <http://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID. For example, <http://handle.itu.int/11.1002/1000/11830-en>.

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 2018

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 and acronyms	2
4	Overview.....	2
	4.1 Characteristics of the SMTTO	2
	4.2 Implementation of information security management for SMTTOs	3
	4.3 Structure of the guidance	3
5	Security policy	4
	5.1 Management direction for information security	4
6	Organization of information security.....	4
	6.1 Internal organization.....	4
	6.2 Mobile devices and teleworking.....	5
7	Human resource security	6
	7.1 Prior to employment	6
	7.2 During employment.....	6
	7.3 Termination and change of employment	7
8	Asset management	8
	8.1 Responsibility for assets	8
	8.2 Information classification	8
	8.3 Media handling.....	9
9	Access control.....	9
	9.1 Business requirements of access control	9
	9.2 User access management	10
	9.3 User responsibilities	11
	9.4 System and application access control	11
10	Cryptography	11
	10.1 Cryptographic controls	11
11	Physical and environmental security	12
	11.1 Secure areas	12
	11.2 Equipment.....	13
12	Operations security	14
	12.1 Operational procedures and responsibilities.....	14
	12.2 Protection from malware	15
	12.3 Backup.....	16
	12.4 Logging and monitoring	16



Documents

Document Sharing Hub

Rec. ITU-T X.1053 (11/2017)

iii

12.5	Control of operational software	16
12.6	Technical vulnerability management	17
12.7	Information systems audit considerations	17
13	Communications security	17
13.1	Network security management	17
13.2	Information transfer	18
14	System acquisition, development and maintenance	18
14.1	Security requirements of information systems	18
14.2	Security in development and support processes	19
14.3	Test data.....	19
15	Supplier relationships	20
15.1	Information security in supplier relationships	20
15.2	Supplier service delivery management.....	20
16	Information security incident management	20
16.1	Management of information security incidents	20
17	Information security aspects of business continuity management	21
17.1	Information security continuity	21
17.2	Redundancies.....	22
18	Compliance	22
18.1	Compliance with legal and contractual requirements	22
18.2	Information security reviews	22
	Annex A – Telecommunication extended control set.....	24
	TEL.9 Access control.....	24
	TEL.9.5 Network access control.....	24
	TEL.11 Physical and environmental security	24
	TEL.11.1 Secure areas.....	24
	TEL.11.3 Security under the control of other party.....	24
	TEL.13 Communications security.....	24
	TEL.13.1 Network security management.....	24
	TEL.18 Compliance	25
	TEL.18.1 Compliance with legal and contractual requirements	25
	Bibliography.....	26

Introduction

Small and medium-sized telecommunication organizations (SMTOs) typically spend little time considering how to manage information security and how to implement security controls, even though they face the same security threats and vulnerabilities as large telecommunication organizations. SMTOs should ensure that appropriate security considerations be adopted to minimize business risk and to ensure information security of their contracts and service level agreements (SLAs).

Recommendation ITU-T X.1053 provides guidelines for the implementation of information security management (ISM) that targets SMTOs based on Recommendation ITU-T X.1051, *Information technology – Security techniques – Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations*.

Security features (confidentiality, integrity, and availability) and terminologies used in this Recommendation are in line with those used in Recommendation ITU-T X.1051.

In order to provide telecommunication services, even in SMTOs, telecommunication organizations need to interconnect and/or share their telecommunication services and facilities, and/or use the telecommunication services and facilities of other telecommunication organizations. Therefore, the management of information security in telecommunication organizations is mutually dependent, and may include any and all areas of network infrastructure, services applications and other facilities.

Regardless of operational scale, service areas, service types, or number of employees, telecommunication organizations should implement appropriate controls to ensure confidentiality, integrity, availability, and any other security property of telecommunication.

This Recommendation provides SMTOs, and those responsible for information security, together with security vendors, auditors, telecommunication terminal vendors, and application content providers, with a common set of general security control objectives based on Recommendation ITU-T X.1051. It further provides these organizations with specific controls and information security management guidelines that allow for the selection and implementation of such controls.



Recommendation ITU-T X.1053

Code of practice for information security controls based on ITU-T X.1051 for small and medium-sized telecommunication organizations

1 Scope

This Recommendation defines guidelines supporting the implementation of information security controls in small and medium-sized telecommunication organizations (SMTOs) based on [ITU-T X.1051] and [ISO/IEC 27002].

The adoption of this Recommendation will allow SMTOs to meet baseline security requirements of confidentiality, integrity, availability, and any other relevant security property specific to these organizations.

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 (2016) | ISO/IEC 27011:2016, *Information technology – Security techniques – Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations*.

[ISO/IEC 27002] ISO/IEC 27002:2013, *Information technology – Security techniques – Code of practice for information security controls*.

3 Definitions and abbreviations

3.1 Definitions

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

3.1.1 confidentiality or non-disclosure agreement: A legal contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes.

3.1.2 data centre: A facility used to house computer systems and associated components, such as telecommunication and storage systems.

3.1.3 outsourcing: When an enterprise contracts out one or more of its internal processes and/or functions to an outside company. Outsourcing moves enterprise resources to an outside enterprise and keeps a retained capability to manage the relationship with the outsourced processes.

3.1.4 parent company: A company that owns enough voting stock in another firm to control management and operations by influencing or electing its board of directors.

3.1.5 small and medium-sized telecommunication organization: A telecommunication organization classified as a small and medium-sized business in accordance with the legislation or the regulations of the country or region in which the business is registered.

3.2 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CEO	Chief Executive Officer
CISO	Chief Information Security Officer
DMZ	Demilitarized Zone
IT	Information Technology
PII	Personally Identifiable Information
SLA	Service Level Agreement
SME	Small Medium Enterprise
SMTO	Small and Medium-sized Telecommunication Organization

4 Overview

4.1 Characteristics of the SMTO

A small and medium-sized telecommunication organization (SMTO) is generally defined according to certain criteria such as the number of employees, sales figures and asset scales (see Annex A).

In contrast to large organizations, SMTOs typically face difficulties in the implementation of information security controls due to limited resources (e.g., limitations of funds, manpower, skills and technology capacity). These can commonly be seen in the following ways:

- a) the size and organization of SMTOs normally means that they do not have sufficient resources to focus on security issues in a full-time capacity, and that consequently security issues are often dealt with in parallel with other business tasks and functions. Since primary tasks handle other business functions and processes as a priority, security issues are often seen as a secondary task with low priority;
- b) the development and deployment of standardized business procedures or standards for information security by SMTOs are often not as extensive or effective as in large organizations due to manpower restrictions;
- c) the specified definition of information security in business processes is very often deficient or entirely lacking;
- d) SMTOs generally have limited experience in the use of technology-based solutions, business applications and processes, and the storage and utilization of information. They tend to depend on limited executive experience and skills;
- e) awareness of information security is often insufficient and information security policies are scarcely established. SMTOs sometimes fail to focus on some of the basic elements of an information security management system, such as identification of assets, risk assessments, access control and countermeasures for security incidents;
- f) SMTOs feature greater chief executive officer (CEO)-centred decision making, making patterns in comparison with business as a whole. Therefore, SMTOs need simpler and more optimized (simplification of existing information security management system) information security activities; and
- g) while large organizations tend to be capable of establishing their own internal expertise and developing and deploying more consistent information security management system by themselves, SMTOs find difficulty in procuring the correct expertise internally. An SMTO generally needs help from external professionals/institutions to deal with the main body of its security activities.

4.2 Implementation of information security management for SMTOs

4.2.1 Security considerations for SMTOs

The requirement for a generic security framework in an SMTO has originated from different sources:

- a) customers/subscribers require confidence in the network and the services to be provided, including the availability, integrity and confidentiality of services according to the customer/subscriber service level agreement (SLA); and
- b) network operators and service providers themselves require security to safeguard their own operational and business interests, as well as public and national infrastructure interests, and to meet their contractual obligations to their customers and their own suppliers (and public interests in general where necessary).

For an SMTO to protect information assets from different sources and under various telecommunication environments, security guidelines, policies and procedures and key activities to support the effective implementation of information security management are indispensable in an SMTO.

The security guidelines should be applicable to the following:

- a) SMTO seeking a business advantage and investment opportunity through the implementation of an information security management system;
- b) SMTO seeking the confidence and assurance that the information security requirements of their interested parties (e.g., suppliers, customers, regulators) will be satisfied;
- c) users and suppliers of the information security-related products and services for the SMTO;
- d) those parties, internal or external to the SMTO, who assess and audit the information security management system for conformity with the requirements of [b-ISO/IEC 27001]; and
- e) those internal or external parties to the SMTO who give advice or training on the information security management system appropriate to that organization.

4.2.2 Design principles of implementation guidance for SMTOs

This Recommendation is structured in line with the format of [ITU-T X.1051] and/or [ISO/IEC 27002]. Considering the situations of SMTOs, there are four cases to provide control and implementation guidance:

- a) in cases where controls specified in [ITU-T X.1051] are applicable without a need for any additional information, only a reference is provided to [ITU-T X.1051] and/or [ISO/IEC 27002];
- b) in cases where controls are not necessarily required for SMTOs, only a reference is provided for information purposes;
- c) in cases where controls do not need all of the implementation guidance in [ITU-T X.1051], the SMTO implementation guidance was constructed by removing unnecessary parts from the original [ITU-T X.1051] implementation guidance text; and
- d) in cases where controls need some implementation guidance applicable to SMTOs, new guidance is provided as SMTO implementation guidance.

4.3 Structure of the guidance

The structure of this Recommendation is as follows:

- Clause 4 describes the security aspects of SMTOs to be considered for the effective implementations of information security controls; and
- Clauses 5 to 18 provide specific controls for SMTOs based on [ITU-T X.1051]. Each clause has the following internal structure:
 - a) a control objective, which states what is to be achieved;