

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1055

(11/2008)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Telecommunication security

Risk management and risk profile guidelines for telecommunication organizations

Recommendation ITU-T X.1055

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

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

Recommendation ITU-T X.1055

Risk management and risk profile guidelines for telecommunication organizations

Summary

Recommendation ITU-T X.1055 describes and recommends the processes, techniques and functional profiles for information security risk management for telecommunication to support Recommendation ITU-T X.1051 | ISO/IEC 27011 and other ITU-T Recommendations. These processes and techniques can be used to assess security requirements and risks identified in telecommunication, and help to select, implement and maintain/update appropriate information security risk controls, i.e., the correct information security level. There are many specific methodologies that have been developed to address the requirements for risk management. This Recommendation provides the criteria for assessing and selecting appropriate methodologies for a telecommunication organization. However, this does not aim to propose a specific risk management methodology for telecommunication. In addition, this Recommendation provides several risk profiles both in terms of ITU-T X.1051 management areas as well as telecom specific services areas.

Source

Recommendation ITU-T X.1055 was approved on 13 November 2008 by ITU-T Study Group 17 (2009-2012) under Recommendation ITU-T A.8 procedure.

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 2009

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

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 and acronyms	1
5	Conventions	2
6	Risk management	2
6.1	Process.....	2
6.2	Risk categories.....	3
6.3	Risk components	4
6.4	Risk assessment and risk treatment	8
7	Risk profiles.....	9
7.1	Definition.....	9
7.2	Use of profiles	9
7.3	Risk profile hierarchy	9
7.4	Profile template	10
7.5	Development and maintenance of risk profiles	11
	Annex A – Risk profile example	12
	Bibliography.....	13

Introduction

Information security risks need to be managed effectively to ensure that organizations and their business is suitably protected from a range of threats. In today's world, telecommunication organizations are operating in a highly dynamic, open and global market place where the boundaries between ICT, services and applications are becoming less defined, with greater complexity and options for information sharing and transfer, on-line business and mobile and wireless services. This computing and networking environment is open to a growing number of risks and threats that can have a dire impact on organizations and their business. Risks to telecommunication networks and services pose growing security threats to telecommunication providers, network and Internet service providers as well as to the businesses and the national infrastructure. This Recommendation provides an overview of the risks that need to be addressed and suitable protections that may be put in place to manage the risks.

Recommendation ITU-T X.1055

Risk management and risk profile guidelines for telecommunication organizations

1 Scope

This Recommendation provides information and advice relevant to the management of information security risks in telecommunication 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 (2008) | ISO/IEC 27011:2008, *Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*.
<<http://www.itu.int/rec/T-REC-X.1051>>

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 impact [b-ISO/IEC 27005]: Adverse change to the level of business objectives achieved.

3.1.2 information security risk [b-ISO/IEC 27005]: The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the likelihood of an event and its consequence.

3.1.3 security incident [b-ITU-T E.409]: A security incident is any adverse event whereby some aspect of security could be threatened.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 risk profile: A set of information describing one of the risks identified by a telecommunication organization.

3.2.2 risk of exposure (RoE): Likelihood of a threat being able to expose one or more system vulnerabilities.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ADSL	Asymmetric Digital Subscriber Line
ASP	Application Service Provider
CATV	Cable Television