

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1059

(10/2019)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Information and network security – Security management

Implementation guidance for telecommunication organizations on risk management of their assets globally accessible in IP-based networks

Recommendation ITU-T X.1059

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
Distributed ledger technology security	X.1430–X.1449
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
QUANTUM COMMUNICATION	X.1700–X.1729

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

Recommendation ITU-T X.1059

Implementation guidance for telecommunication organizations on risk management of their assets globally accessible in IP-based networks

Summary

Recommendation ITU-T X.1059 provides guidance for telecommunication organizations on the risk management of their assets globally accessible in IP-based networks, the assets which are exposed directly to hackers and attackers. These assets may also be connected to the traditional (and even old) assets of legacy telecommunication networks, which might have some design level vulnerabilities that could be difficult to fix. Therefore, it would be practical to consider all the assets globally accessible in IP-based networks (AGIT) of a telecommunication organization as a whole, and to introduce some specific security controls to continuously reduce the overall risks and to strengthen the overall security of telecommunication services and networks.

It is suggested that the proposed controls be applied with high priority to assets globally accessible in IP-based networks. The controls might also be applicable to other assets.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1059	2019-10-29	17	11.1002/1000/14045

Keywords

Assets survey, risk identification, risk management.

* 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 2020

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 and acronyms	2
5	Conventions	2
6	Overview of risk management for AGIT.....	2
	6.1 Processes.....	2
	6.2 Phases and steps	3
	6.3 Structure of the description of the AGIT risk management process	4
7	Risk assessment	5
	7.1 Risk identification	5
	7.2 Risk analysis	9
8	Risk evaluation	10
	8.1 Description	10
9	Risk treatment.....	11
	9.1 Overview	11
	9.2 Emergent treatment	11
	9.3 Regular treatment	12
10	Monitoring and review	12
	10.1 Description	12
	10.2 Implementation guidance	12
11	Communication and consultation	13
	11.1 Description	13
	11.2 Implementation guidance	13
12	Recording and reporting	13
	12.1 Description	13
	12.2 Implementation guidance	13
	Bibliography.....	15

Introduction

Telecommunication organizations have become more progressive to leverage the benefits of both legacy and Internet services. Some of these organizations have transferred their legacy services to the Internet, such as using Internet protocol (IP) technology to provide voice services instead of using circuit-switched technology and even integrating voice services such as voice over long-term evolution (VoLTE) with ordinary voice over IP (VoIP). Some organizations have merged Internet flexibility into legacy services, for example, by enabling customers to use web portals to send messages out to the mobile terminals or to check messages and missed calls. Some organizations also utilize the Internet to provide customer self-service experiences, for example, by allowing customers to update their contracts and to make transactions online.

During this transformation process, a large number of assets are deployed by telecommunication organizations to bridge the physical network boundary between IP-based networks and telecommunication networks capabilities. Securing these assets, globally accessible in IP-based networks, has become one of the most obvious challenges for security management teams and the risk management of these assets could be a priority or primary concern for telecommunication organizations.

Recommendation ITU-T X.1059

Implementation guidance for telecommunication organizations on risk management of their assets globally accessible in IP-based networks

1 Scope

This Recommendation identifies threats and challenges that could arise when telecommunication network assets are globally accessible in IP-based networks. It also provides best practices and guidance for the implementation of security controls for the risk management of these assets.

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.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 control [b-ISO/IEC 27000]: Measure that is modifying risk.

NOTE 1 – Controls include any process, policy, device, practice, or other actions which modify risk.

NOTE 2 – Controls may not always exert the intended or assumed modifying effect.

3.1.2 impact [b-ITU-T X.1055]: Adverse change to the level of business objectives achieved.

3.1.3 risk profile [b-ITU-T X.1055]: A set of information describing one of the risks identified by a telecommunication organization.

3.1.4 risk of exposure [b-ITU-T X.1055]: Likelihood of a threat being able to expose one or more system vulnerabilities.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 assets globally accessible in IP-based network: Hardware and software assets that can be reached or connected by an Internet protocol (IP) or a uniform resource locator (URL) address or a certain client, etc., through the infrastructure of public IP networks.

3.2.2 AGIT profile: A set of information describing an asset globally accessible in IP-based networks for telecommunication organizations (AGIT) identified as belonging to a telecommunication organization.

3.2.3 residual risk: An old risk that cannot disappear or a new risk that appears after risk treatment.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AGIT	Assets Globally accessible in IP-based network for Telecommunication organizations
DDoS	Distributed Denial of Service
IP	Internet Protocol
IT	Information Technology
OS	Operating System
PII	Personally Identifiable Information
RoE	Risk of Exposure
SMS	Short Message Service
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VoIP	Voice over IP
VoLTE	Voice over Long-Term Evolution
VPN	Virtual Private Network
WWW	World Wide Web

5 Conventions

None.

6 Overview of risk management for AGIT

This Recommendation provides implementation guidance of risk management for a specified category of assets which are globally accessible in IP-based network (AGIT) as defined in clause 3.2.1.

6.1 Processes

In general, assets globally accessible in IP-based network for telecommunication organizations (AGIT) include the following six risk management processes (see Figure 6-1):

- 1) Risk assessment
- 2) Risk evaluation
- 3) Risk treatment
- 4) Monitoring and review
- 5) Communication and consultation
- 6) Recording and reporting

As part of the risk management lifecycle, AGIT risk management processes from 1 to 3 should be executed in a pre-defined order. The processes of 5, 6 and 7 should provide a feedback mechanism and should work in parallel throughout the whole cycle as shown in Figure 6-1.