

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1642

(03/2016)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Cloud computing security – Cloud computing security best
practices and guidelines

Guidelines for the operational security of cloud computing

Recommendation ITU-T X.1642

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	
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
PKI related Recommendations	X.1340–X.1349
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.1642

Guidelines for the operational security of cloud computing

Summary

Recommendation ITU-T X.1642 provides generic operational security guidelines for cloud computing from the perspective of cloud service providers (CSPs). It analyses the security requirements and metrics for the operation of cloud computing. A set of security measures and detailed security activities for the daily operation and maintenance are provided to help CSPs mitigate security risks and address security challenges for the operation of cloud computing.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1642	2016-03-23	17	11.1002/1000/12616

Keywords

Cloud computing, operational security, security clause of the service level agreement (SLA).

* 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 2016

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.....	2
4 Abbreviations and acronyms	2
5 Conventions	3
6 Overview.....	3
7 Requirements of the security clause of the service level agreement	4
7.1 Security responsibility between CSPs and CSCs	4
7.2 Requirements of the security clause of SLA	5
8 Guidelines of daily operational security	7
8.1 Identity management and access control	8
8.2 Data encryption and key management	9
8.3 System security monitoring	10
8.4 Disaster recovery	11
8.5 Security configuration management.....	11
8.6 Security event processing	13
8.7 Patch upgrade	14
8.8 Securing configuration management	16
8.9 Emergency response plans	17
8.10 Backup.....	18
8.11 Internal security audit.....	20
Bibliography.....	22

1

Recommendation ITU-T X.1642

Guidelines for the operational security of cloud computing

1 Scope

This Recommendation clarifies the security responsibilities between cloud service providers (CSPs) and cloud service customers (CSCs), and analyses the requirements and categories of security metrics of operational security for cloud computing. It defines sets of detailed security measures and security activities for the daily operation and maintenance for cloud computing services and infrastructure from the perspective of CSPs, to fulfil the requirements of operational security for cloud computing.

This Recommendation will be helpful for CSPs to reduce operational risks. The target audiences of this Recommendation are CSPs, such as traditional telecommunication operators and Internet service providers (ISPs).

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 cloud computing [b-ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

3.1.2 cloud service [b-ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.3 cloud service customer [b-ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

3.1.4 cloud service partner [b-ITU-T Y.3500]: Party which is engaged in support of, or auxiliary to, activities of either the cloud service provider or the cloud service customer, or both.

3.1.5 cloud service provider [b-ITU-T Y.3500]: Party which makes cloud services available.

3.1.6 infrastructure as a service (IaaS) [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer is an infrastructure capabilities type.

3.1.7 multi-tenancy [b-ITU-T Y.3500]: Allocation of physical or virtual resources such that multiple tenants and their computations and data are isolated from and inaccessible to one another.

3.1.8 network as a service (NaaS) [b-ITU-T Y.3500]: Cloud service category in which the capability provided to the cloud service customer is transport connectivity and related network capabilities.

3.1.9 party [b-ISO 27729]: Natural person or legal person, whether or not incorporated, or a group of either.

3.1.10 platform as a service (PaaS) [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the service customer is a platform capabilities type.

3.1.11 security challenge [b-ITU-T X.1601]: A security "difficulty" other than a direct security threat arising from the nature and operating environment of cloud services, including "indirect" threats.

3.1.12 security domain [b-ITU-T X.810]: A set of elements, a security policy, a security authority and a set of security-relevant activities in which the set of elements are subject to the security policy for the specified activities, and the security policy is administered by the security authority for the security domain.

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

3.1.14 service level agreement (SLA) [b-ISO/IEC 20000-1]: Documented agreement between the service provider and customer that identifies services and service targets.

3.1.15 software as a service (SaaS) [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer is an application capabilities type.

3.1.16 tenant [b-ITU-T Y.3500]: One or more cloud service users sharing access to a set of physical and virtual resources.

3.1.17 threat [b-ISO/IEC 27000]: Potential cause of an unwanted incident, which may result in harm to a system or organization.

3.1.18 vulnerability [b-NIST-SP-800-30]: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ACL	Access Control List
API	Application Programming Interface
BIA	Business Impact Analysis
CCTV	Closed Circuit Television
CPU	Central Processing Unit
CSC	Cloud Service Customer
CSN	Cloud Service Partner
CSP	Cloud Service Provider
DB	Database
DDoS	Distributed Denial of Service
DLP	Data Leakage Prevention
DoS	Denial of Service
IAM	Identity and Access Management
IaaS	Infrastructure as a Service
ICT	Information and Communication Technology
IdM	Identity Management

IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
ISP	Internet Service Provider
IT	Information Technology
JIT	Just In Time
LDAP	Lightweight Directory Access Protocol
NaaS	Network as a Service
OS	Operating System
PaaS	Platform as a Service
RPO	Recovery Point Objective
RTO	Recovery Time Objectives
SaaS	Software as a Service
SLA	Service Level Agreement
SMS	Short Message Service
SSO	Single Sign-On
VDC	Virtual Data Centre
VM	Virtual Machine

5 Conventions

None.

6 Overview

With the rapid expansion of the cloud computing market and the establishment of industry chains, security issues continue to be a major and important topic that cannot be ignored. Cloud computing systems are facing more challenges than traditional information technology (IT) systems because they are more complicated, and huge amounts of users' private data have been stored in the cloud. Both security and privacy protection are the most important factors when customers evaluate the use of cloud computing services.

More and more cloud services will be supplied, and methods to guarantee the reliability of these cloud services have become more urgent. It is therefore necessary to thoroughly investigate the operational security of cloud computing to provide guidelines for cloud service providers (CSPs). The guidelines can help CSPs reduce the security risk from improper operation, unreasonable business design, etc., and improve the overall security level of operation for cloud computing services.

From the perspective of CSPs, the main security challenges of operational security are described below:

- 1) Challenges to the maintenance of cloud computing infrastructure: When cloud computing provides the users with IT infrastructure, a platform or software as a service, the stability, reliability and safe delivery of cloud services are a prerequisite to carry out business. In order to guarantee that customer service is not interrupted, the infrastructure of the cloud system should be ensured for a reliable and stable operation, and the necessary precautions should be adopted to protect the safety and privacy of user's information. Even in the event of a small