

COMMITTEE DRAFT		Reference number:	
ISO/IEC 1st CD 27017		ISO/IEC JTC 1/SC 27 N13160	
Date: 2013-12-11		Supersedes document SC 27 N12429	
THIS DOCUMENT IS STILL UNDER STUDY AND SUBJECT TO CHANGE. IT SHOULD NOT BE USED FOR REFERENCE PURPOSES.			
ISO/IEC JTC 1/SC 27 Information technology - Security techniques Secretariat: Germany (DIN)	Circulated to P- and O-members, and to technical committees and organizations in liaison for comments by: 2014-03-12 Please submit your comments via the online balloting application by the due date indicated.		
ISO/IEC 1st CD 27017			
Title: Information technology -- Security techniques --Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002			
Project: 1.27.91 (27017)			
Explanatory Report			
Status	SC 27 Decision	Reference documents	
		Input	Output
<i>For information regarding previous development stages please see the 2nd page of this report.</i>			
ISO/IEC 27017 4th WD	45 th WG 1 meeting, Oct. 2012, resolutions 1, 8, 15, 16, 21*, 26 (N11900). * <i>appointment of ITU-T SG editor</i>	SoCom (N11470); CSA (N11586); ISACA (N11587); ITU-T SG17 (N11474).	60-day LB/SoV on change TS ->IS (N12077/N12180); Request/endorsement title change (N12145/N12184); Liaisons to: CSA (N11885); ITU-T FG Cloud (N11889); JTC 1/SC 38 (N11899); Meet. report (N12017); DoC (N11915); Text f. 4 th WD (N11916).
ISO/IEC 27017 5th WD	46 th WG 1 meeting, Oct. 2013, resolutions 1, 2, 5 (N12440); Del. of Auth. f. 1 st CD as per resolution 13 of 25 th SC 27 Plenary, April 2013 (N12739).	SoCom (N12294); ISACA com. (N12179) ITU-T SG17 liaison (N12275); Draft DoC (N12355).	Liaisons to: ISACA (N12515); ITU-T SG17 (N12507); DoC (N12767, replaces N12428); Text f. 5 th WD (N12429).
ISO/IEC 27017 1st CD	47 th WG 1 meeting, Oct. 2013, resolutions 1, 12, 26 (N13440)	SoCom (N12887); CA com. (N13068); ISACA com. (N12893); ITU-T SG17 liaison + com. (N12894); Draft DoC (N13107)..	Request/endorsement limit dates extension (N13448 / N13nnn1); Liaison to: ITU-T SG 17 (N13174); DoC (N13159); Text f. 1 st CD (N13160).
CD Registration and Consideration			
In accordance with resolution 12 (see SC 27 N13440) of the 47 th SC 27/WG1 Plenary meeting held in Incheon, Republic of Korea, 25 th October 2013 the hereby attached document has been registered with the ISO Central Secretariat (ITTF) as a 1st Committee Draft (CD) and is herewith being circulated for a 1 st Committee Draft (CD) letter ballot closing by			
2014-03-12			
MEDIUM: http://isotc.iso.org/livelink/livelink/open/jtc1sc27			
NO OF PAGES: 2 + 57			

Explanatory Report (2 nd page)			
Status	SC 27 Decision	Reference documents	
		Input	Output
Joint WG1/475 study period on cloud computing security and privacy	41 st WG 1, 4, 5 meetings, Oct. 2010, resolutions (N9420, N9084, N9402)	GB rapporteur nomin. (N9442); JP contr. (N9044); JP present. (N9410); ISACA contr. (N9542); ISF contr. (N9408); ITU-T SG 17 liaison + contr. (N9470).	Call f. contr. (N9471).
NWIP 1st WD	42 nd WG 1 meeting, April 2011, resolutions 1, 4 (N10100); 22 nd SC 27 Plenary April 2011, resolution 20 (N10101)..	US contr. (N9850, N9851). ITU-T FG Cloud liaison (N10073).	SP reports(N10027, N10028); Future direction (N10036); Call f. contr. (N10035); NWIP (N10029).
ISO/IEC NP 27017 2nd WD	43 rd WG 1 meeting, Oct. 2011, resolutions 1, 4, 25 (N10570).	BE contr. (N10119); ITU-T SG 17 liaison + contr. (N10339). JTC 1/SC 7 li. + com. (N10201); SP report (N10220); SoV (N10212).	Liaisons to: ITU-T FG Cloud (N10600); DoC (N10593); Text f. 2 nd WD (N10594).
ISO/IEC NP 27017 2nd WD	43 rd WG 1 meeting, Oct. 2011, resolutions 1, 4, 25 (N10570).	BE contr. (N10119); JTC 1/SC 7 li. + com. (N10201); SoV (N10212).	Liaisons to: ITU-T FG Cloud (N10600); DoC (N10593); Text f. 2 nd WD (N10594).
ISO/IEC 27017 3rd WD	44 th WG 1 meeting, May 2012, resolutions 1, 6, 22, 26 (N11101). 24 th SC P (N11101).	SoCom (N10830); INLAC com. (N10963); ISACA (N10927); ITUT FG Cloud (N10678); AU (N10966); SG (N11065); SoC (N10830); Draft DoC (N11068).	Liaisons to: CSA (N11140); INLAC (N11132); ISF (N11141); ITU-T SG 13 (N11153); ITU-T SG 17 (N11135); ITU-T FG Cloud (N11139); Meet. rep (N11124); DoC (N11121); Text f. 3 rd WD (N11122).

Information technology – Security techniques – Code of practice for information security controls for cloud computing services based on ISO/IEC 27002

Copyright notice

This ISO document is a working draft or committee draft and is copyright-protected by ISO. While the reproduction of working drafts or committee drafts in any form for use by participants in the ISO standards development process is permitted without prior permission from ISO, neither this document nor any extract from it may be reproduced, stored or transmitted in any form for any other purpose without prior written permission from ISO.

Requests for permission to reproduce this document for the purpose of selling it should be addressed as shown below or to ISO's member body in the country of the requester:

Secretariat of ISO/IEC JTC 1/SC 27
DIN German Institute for Standardization
DE-10772 Berlin

Tel. + 49 30 2601 2652

Fax + 49 30 2601 4 2652

E-mail krystyna.passia@din.de

Web <http://www.jtc1sc27.din.de/en> (public web site)

<http://isotc.iso.org/isotcportal/index.html> (SC27 documents)

Reproduction for sales purposes may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

ITU-T RECOMMENDATION X.nnnn

INTERNATIONAL STANDARD ISO/IEC 27017

Information technology – Security techniques – Code of practice for information security controls for cloud computing services based on ISO/IEC 27002

Summary

This Recommendation | International Standard provides guidelines for information security controls applicable to the use and provisioning of cloud services by providing:

- additional implementation guidance for relevant controls specified in ISO/IEC 27002; and,
- additional controls with implementation guidance that specifically relate to cloud services.

This Recommendation | International Standard provides implementation guidance for both providers and customers of cloud services.

Contents

0	Introduction	xi
1	Scope	1
2	Normative references	1
3	Definitions and abbreviations	1
3.1	Terms and definitions	1
3.2	Abbreviations	3
4	Cloud sector-specific concepts	4
4.1	Overview	4
4.2	Supplier relationships in cloud services	4
4.3	Relationships between cloud service customers and cloud service providers	5
4.4	Assessing information security risks in cloud services	5
4.5	Structure of this standard	5
5	Information security policies	7
5.1	Management direction for information security	7
5.1.1	Policies for information security	7
5.1.2	Review of the policies for information security	8
6	Organization of information security	9
6.1	Internal organization	9
6.1.1	Information security roles and responsibilities	9
6.1.2	Segregation of duties	9
6.1.3	Contact with authorities	9
6.1.4	Contact with special interest groups	9
6.1.5	Information security in project management	10
6.2	Mobile devices and teleworking	10
6.2.1	Mobile device policy	10
6.2.2	Teleworking	10
7	Human resource security	11
7.1	Prior to employment	11
7.1.1	Screening	11
7.1.2	Terms and conditions of employment	11
7.2	During employment	11
7.2.1	Management responsibilities	11
7.2.2	Information security awareness, education and training	11
7.2.3	Disciplinary process	12
7.3	Termination and change of employment	12
7.3.1	Termination or change of employment responsibilities	12
8	Asset management	13

8.1	Responsibility for assets	13
8.1.1	Inventory of assets	13
8.1.2	Ownership of assets	13
8.1.3	Acceptable use of assets	13
8.1.4	Return of assets	13
8.2	Information classification	14
8.2.1	Classification of information	14
8.2.2	Labelling of information	14
8.2.3	Handling of assets	14
8.3	Media handling	14
8.3.1	Management of removable media	14
8.3.2	Disposal of media	14
8.3.3	Physical media transfer	14
9	Access control	15
9.1	Business requirements of access control	15
9.1.1	Access control policy	15
9.1.2	Access to networks and network services	15
9.2	User access management	15
9.2.1	User registration and de-registration	15
9.2.2	User access provisioning	15
9.2.3	Management of privileged access rights	15
9.2.4	Management of secret authentication information of users	16
9.2.5	Review of user access rights	16
9.2.6	Removal or adjustment of access rights	16
9.3	User responsibilities	16
9.3.1	Use of secret authentication information	16
9.4	System and application access control	16
9.4.1	Information access restriction	16
9.4.2	Secure log-on procedures	17
9.4.3	Password management system	17
9.4.4	Use of privileged utility programs	17
9.4.5	Access control to program source code	17
10	Cryptography	18
10.1	Cryptographic controls	18
10.1.1	Policy on the use of cryptographic controls	18
10.1.2	Key management	18
11	Physical and environmental security	20
11.1	Secure areas	20
11.1.1	Physical security perimeter	20
11.1.2	Physical entry controls	20
11.1.3	Securing offices, rooms and facilities	20

11.1.4	Protecting against external and environmental threats	20
11.1.5	Working in secure areas	20
11.1.6	Delivery and loading areas	20
11.2	Equipment	20
11.2.1	Equipment siting and protection	20
11.2.2	Supporting utilities	20
11.2.3	Cabling security	20
11.2.4	Equipment maintenance	21
11.2.5	Removal of assets	21
11.2.6	Security of equipment and assets off-premises	21
11.2.7	Secure disposal or re-use of equipment	21
11.2.8	Unattended user equipment	21
11.2.9	Clear desk and clear screen policy	21
12	Operations security	22
12.1	Operational procedures and responsibilities	22
12.1.1	Documented operating procedures	22
12.1.2	Change management	22
12.1.3	Capacity management	22
12.1.4	Separation of development, testing and operational environments	23
12.2	Protection from malware	23
12.2.1	Controls against malware	24
12.3	Backup	24
12.3.1	Information backup	24
12.4	Logging and monitoring	24
12.4.1	Event logging	24
12.4.2	Protection of log information	25
12.4.3	Administrator and operator logs	25
12.4.4	Clock synchronisation	25
12.5	Control of operational software	25
12.5.1	Installation of software on operational systems	26
12.6	Technical vulnerability management	26
12.6.1	Management of technical vulnerabilities	26
12.6.2	Restrictions on software installation	26
12.7	Information systems audit considerations	26
12.7.1	Information systems audit controls	26
13	Communications security	28
13.1	Network security management	28
13.1.1	Network controls	28
13.1.2	Security of network services	28
13.1.3	Segregation in networks	28
13.2	Information transfer	28

13.2.1	Information transfer policies and procedures	28
13.2.2	Agreements on information transfer	28
13.2.3	Electronic messaging.....	29
13.2.4	Confidentiality or non-disclosure agreements	29
14	System acquisition, development and maintenance	30
14.1	Security requirements of information systems	30
14.1.1	Security requirements analysis and specification	30
14.1.2	Securing applications services on public networks	30
14.1.3	Protecting application services transactions.....	30
14.2	Security in development and support processes.....	30
14.2.1	Secure development policy.....	30
14.2.2	System change control procedures	30
14.2.3	Technical review of applications after operating platform changes.....	31
14.2.4	Restrictions on changes to software packages	31
14.2.5	Secure system engineering principles	31
14.2.6	Secure development environment.....	31
14.2.7	Outsourced development.....	31
14.2.8	System security testing.....	31
14.2.9	System acceptance testing.....	31
14.3	Test data.....	31
14.3.1	Protection of test data	31
15	Supplier relationships	32
15.1	Security in supplier relationship.....	32
15.1.1	Information security policy for supplier relationships	32
15.1.2	Addressing security within supplier agreements	32
15.1.3	Information and communication technology supply chain	33
15.2	Supplier service delivery management	33
15.2.1	Monitoring and review of supplier services.....	33
15.2.2	Managing changes to supplier services.....	33
16	Information security incident management	34
16.1	Management of information security incidents and improvements	34
16.1.1	Responsibilities and procedures.....	34
16.1.2	Reporting information security events	34
16.1.3	Reporting information security weaknesses	34
16.1.4	Assessment of and decision on information security events	35
16.1.5	Response to information security incidents	35
16.1.6	Learning from information security incidents	35
16.1.7	Collection of evidence.....	35
17	Information security aspects of business continuity management.....	36
17.1	Information security continuity	36
17.1.1	Planning information security continuity	36

17.1.2	Implementing information security continuity	36
17.1.3	Verify, review and evaluate information security continuity	36
17.2	Redundancies	36
17.2.1	Availability of information processing facilities	36
18	Compliance	37
18.1	Compliance with legal and contractual requirements	37
18.1.1	Identification of applicable legislation and contractual requirements	37
18.1.2	Intellectual property rights (IPR)	37
18.1.3	Protection of records	37
18.1.4	Privacy and protection of personally identifiable information	37
18.1.5	Regulation of cryptographic controls	38
18.2	Information security reviews	38
18.2.1	Independent review of information security	38
18.2.2	Compliance with security policies and standards	38
18.2.3	Technical compliance review	38
Annex A	Cloud Service Extended Control Set (normative)	39
CLD.6.3	Relationship between cloud service customer and cloud service provider	39
CLD.6.3.1	Demarcation of responsibility	39
CLD.9.5	Access control of cloud service customer's data in shared virtual environment	40
CLD.9.5.1	Segregation in virtual computing environments	40
CLD.12.1	Operations security	41
CLD.12.1.2	Administrator's operational security	41
CLD.12.4	Logging and monitoring	41
CLD.12.4.3	Administrator and operator logs	42
CLD.12.4.5	Monitoring of Cloud Services	42
CLD.13	Communications security	42
CLD.13.1	Network security management	42
CLD.13.1.4	Cooperation of configurations between virtual and physical network	43
Annex B	References on information security risk related cloud computing (informative)	44

Foreword

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. 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 world-wide basis. The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups that, 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 that fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

International Standard ISO/IEC 27017 was prepared by Technical Committee ISO/IEC JTC1 Subcommittee SC 27, *Security techniques*, in collaboration with ITU-T. The identical text is published as ITU-T Recommendation X.nnnn.

0 Introduction

The guidelines contained within this Recommendation | International Standard are in addition to and complement the implementation guidance given in ISO/IEC 27002:2013.

Specifically, this Recommendation | International Standard provides guidelines supporting the implementation of information security controls for cloud service providers and cloud service customers. Selection of appropriate information security controls, and the application of the implementation guidance provided, will depend on a risk assessment as well as any legal, contractual, or regulatory or other Cloud-sector specific information security requirements.

Information Technology — Security Techniques — Code of practice for information security controls for cloud computing services based on ISO/IEC 27002

1 Scope

This Recommendation | International Standard gives guidelines for information security controls applicable to the use and provisioning of cloud services by providing:

- additional implementation guidance for relevant controls specified in ISO/IEC 27002:2013; and,
- additional controls with implementation guidance that specifically relate to cloud services.

This Recommendation | International Standard provides implementation guidance for both providers and customers of cloud services.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology - Security techniques - Information security management systems - Overview and vocabulary*

ISO/IEC 27002:2013, *Information technology - Security techniques - Code of practice for information security controls*

3 Definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and the following apply.

3.1.1

application capabilities type

cloud capabilities type (3.1.3) in which the **cloud service customer** (3.1.7) can use the **cloud service provider's** (3.1.8) applications

[ISO/IEC DIS 17788 | Y.ccdef]

3.1.2

capability

quality of being able to perform a given activity

[ISO 19440:2007]

3.1.3

cloud capability type

classification of the functionality, based on resources used, provided by a **cloud service** (3.1.5) to the **cloud service customer** (3.1.7)

NOTE The cloud capabilities types are **infrastructure capabilities type** (3.1.11), **platform capabilities type** (3.1.14) and **application capabilities type** (3.1.1).

[ISO/IEC DIS 17788 | Y.ccdef]

3.1.4

cloud computing

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

NOTE Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

[ISO/IEC DIS 17788 | Y.ccdef]

3.1.5

cloud service

one or more **capabilities** (3.1.2) offered via **cloud computing** (3.1.4) invoked using a defined interface

[ISO/IEC DIS 17788 | Y.ccdef]

3.1.6

cloud service category

group of **cloud services** (3.1.5) that possess some common set of qualities

NOTE A **cloud service category** can include **capabilities** (3.1.2) from one or more **cloud capabilities types** (3.1.3)

[ISO/IEC DIS 17788 | Y.ccdef]

3.1.7

cloud service customer

party (3.1.13) which is in a business relationship for the purpose of using **cloud services** (3.1.5)

NOTE A business relationship may not necessarily imply financial agreements.

[ISO/IEC DIS 17788 | Y.ccdef]

3.1.8

cloud service provider

party (3.1.13) which makes **cloud services** (3.1.5) available

[ISO/IEC DIS 17788 | Y.ccdef]

3.1.9

cloud service user

natural person, or entity acting on their behalf, associated with a **cloud service customer** (3.1.7) that uses **cloud services** (3.1.5)

NOTE Examples of such entities include devices and applications.

[ISO/IEC DIS 17788 | Y.ccdef]

3.1.10

Infrastructure as a Service (IaaS)

cloud service category (3.1.6) in which the **cloud capabilities type** (3.1.3) provided to the **cloud service customer** (3.1.7) is an **infrastructure capabilities type** (3.1.11)

NOTE The **cloud service customer** (3.1.7) does not manage or control the underlying physical and virtual resources but does have control over operating systems, storage, and deployed applications that use the physical and virtual resources. The **cloud service customer** (3.1.7) may also have limited ability to control certain networking components (e.g., host firewalls).

[ISO/IEC DIS 17788 | Y.ccdef]

3.1.11

Infrastructure capabilities type

cloud capabilities type (3.1.3) in which the **cloud service customer** (3.1.7) can provision and use processing, storage and networking resources

[ISO/IEC DIS 17788 | Y.ccdef]

3.1.12

Platform as a Service (PaaS)

cloud service category (3.1.6) in which the **cloud capabilities type** (3.1.3) provided to the **cloud service customer** (3.1.7) is a **platform capabilities type** (3.1.14)

[ISO/IEC DIS 17788 | Y.ccdef]

3.1.13

party

natural person or legal person, whether or not incorporated, or a group of either

[ISO 27729:2012]

3.1.14

platform capabilities type

cloud capabilities type (3.1.3) in which the **cloud service customer** (3.1.7) can deploy, manage and run customer-created or customer-acquired applications using one or more programming languages and one or more execution environments supported by the **cloud service provider** (3.1.8)

[ISO/IEC DIS 17788 | Y.ccdef]

3.1.15

Software as a Service (SaaS)

cloud service category (3.1.6) in which the **cloud capabilities type** (3.1.3) provided to the **cloud service customer** (3.1.7) is an **application capabilities type** (3.1.1)

[ISO/IEC DIS 17788 | Y.ccdef]

3.1.16

tenant

group of **cloud service users** (3.1.9) sharing access to a set of physical and virtual resources

[ISO/IEC DIS 17788 | Y.ccdef]

3.2 Abbreviations

For the purposes of this document, the following abbreviations apply.

IaaS: Infrastructure as a Service

NDA: non-disclosure agreement

PaaS: Platform as a Service

SaaS: Software as a Service

VLAN: Virtual Local Area Network

4 Cloud sector-specific concepts

4.1 Overview

Fundamentally, cloud computing has changed how organizations should assess and mitigate information security risks because there have been significant changes in how computing resources are technically designed, operated and governed. ISO/IEC 27017 is distinct by providing more relevant implementation guidance based on ISO/IEC 27002 but also supplements additional extended controls to address emerging cloud-specific information security threats and risks considerations.

Users of this Recommendation | International Standard need to use ISO/IEC 27002 and reference its clauses 5 to 18 for controls, implementation guidance and other information. Because of the general applicability of ISO/IEC 27002, many of the controls, implementation guidance and other information are applicable to both the general and cloud computing contexts of the organization. As an example, “6.1.2 Segregation of duties” of ISO/IEC 27002 provides a control that is generally valid in the organization. Additionally, a cloud service customer can derive the requirement of segregation of duties in the cloud environment from the same control, e.g., segregating cloud service administrators and cloud service users. This is an example of interpreting a control of ISO/IEC 27002 in the cloud computing context.

As an extension to ISO/IEC 27002, this Recommendation | International Standard further provides cloud service specific controls, implementation guidance and other information (see 4.6) which are prepared to meet cloud specific risks that accompany the technical and operational features of cloud services (see Annex B). Cloud service customer and cloud service provider can reference ISO/IEC 27002 and this Recommendation | International Standard, and select controls with its implementation from them, and add other controls if necessary. This can be done through the process of information security risk assessment and risk treatment in the organizational and business context where cloud services are used or provided (see 4.5).

4.2 Supplier relationships in cloud services

ISO/IEC 27002 has a clause “15 Supplier relationships” which provides controls, implementation guidance and other information for managing information security in the context of supplier relationships. In relation with this, use and provision of the cloud services are versions of supplier relationships, where the cloud service customer is an acquirer, and the cloud service provider is a supplier. Thus, the clause applies to the cloud service customers and cloud service providers.

Cloud service providers and customers can also form a supply chain. Suppose that a cloud service provider provides an infrastructure capabilities type service. On top of it, another cloud service provider can provide an application capabilities type service. In this case, the second provider is a cloud service customer in relation with the former, and a cloud service provider in relation with the customer of its service. This example illustrates the case where this Recommendation | International Standard is applied to an organization both as a cloud service customer and as cloud service provider. Cloud service customers and cloud service suppliers form a supply chain through service processes, and “15.1.3 Information and communication technology supply chain” of ISO/IEC 27002 applies.

Multi-part International Standard ISO/IEC 27036, information security for supplier relationships, provides detailed guidance on the information security in supplier relationships to the acquirer and supplier of products and services. The standard is also applicable to cloud service customers and cloud service providers.

4.3 Relationships between cloud service customers and cloud service providers

In the cloud computing environment, a cloud service customer's information is stored, transmitted and processed in cloud services, therefore, a cloud service customer's business processes depends upon the availability of a service. Without direct control over a cloud service, the cloud service customer may need to take extra precautions with their information security practices.

Before entering into a supplier relationship, the cloud service customer needs to select cloud services, taking into account the possible gaps between its information security requirements and the levels of information security of the service. Once a cloud service is selected, the cloud service customer is required to manage the cloud service provider's service operations. In these relationships, the cloud service provider is required to provide information and support, which are necessary for the information security of the cloud service customer. When the information security controls provided by a cloud service provider are pre-set and cannot be changed by the cloud service customer, the cloud service customer may need to implement its own, extra controls to mitigate risks.

4.4 Assessing information security risks in cloud services

Information security risks identify information security requirements. Each cloud service customer or cloud service provider is expected to complete its own information security risk assessment to determine the impact to its business in relation to the likelihood of information security exposure or controls failure. Expenditure on controls needs to be balanced against the business harm likely to result from information security failures. The results of the risk assessment help to guide and determine the appropriate management actions and priorities for managing information security risks, and for implementing controls selected to protect against these risks.

Risk assessment should be run periodically, but may also be performed following the manifestation or observation of a vulnerability or new threat.

4.5 Structure of this standard

This Recommendation | International Standard is structured in a format similar to ISO/IEC 27002. This Recommendation | International Standard includes clauses 5 to 18 of ISO/IEC 27002 by stating application of its texts at each sub clause and paragraph.

When objectives and controls specified in ISO/IEC 27002 are applicable without a need for any additional information, only a reference to ISO/IEC 27002 is provided.

When an objective or control with implementation guidance is needed in addition to those of ISO/IEC 27002, they are given in Annex A: Cloud Computing Service Extended Control Set (normative).

When a control needs additional guidance specific to cloud services, the 27002 control is referenced and the reference is then followed by cloud service specific implementation guidance related to the control. Cloud service specific implementation guidance and other information are included in the following clauses:

- Information Security Policies (Clause 5)
- Organization of information security (Clause 6)
- Human Resource Security (Clause 7)
- Asset management (Clause 8)
- Access Control (Clause 9)

- 1 — Cryptography (Clause 10)
- 2 — Physical and environmental security (Clause 11)
- 3 — Operations security (Clause 12)
- 4 — Communications security (Clause 13)
- 5 — Systems acquisition, development and maintenance (Clause 14)
- 6 — Supplier relationships (Clause 15)
- 7 — Information security incident management (Clause 16)
- 8 — Information security aspects of business continuity management (Clause 17)
- 9 — Compliance (Clause 18)

10 Each clause contains one or more of the main security categories.

11 Each main security category contains:

- 12 a) a control objective stating what is to be achieved; and
- 13 b) one or more controls that can be applied to achieve the control objective.

14 Control descriptions are structured as follows:

15 Control objective of ISO/IEC 27002

16 provides the description “The objective specified in clause X.X of ISO/IEC 27002 applies.”

17 Control, Implementation guidance, Other information of ISO/IEC 27002

18 provides the description “Control x.x.x and the associated implementation guidance and other
19 information specified in ISO/IEC 27002 apply.

20 Sector-specific guidance for cloud services

21 provides the description “The following sector-specific guidance also applies.” followed by one of two
22 types of guidance description:

23 Type 1 is used when there is separate guidance for the cloud service customer and the cloud service
24 provider.

25 Type 2 is used when the guidance is the same for both the cloud service customer and cloud service
26 provider.

27 Type 1

Cloud service customer	Cloud service provider

28

1 Type 2

Cloud service customer	Cloud service provider

2

3 Other information for cloud computing

4 provides additional information that may need to be considered.

5 **5 Information security policies**

6 **5.1 Management direction for information security**

7 The objective specified in clause 5.1 of ISO/IEC 27002 applies.

8 **5.1.1 Policies for information security**

9 Control 5.1.1 and the associated implementation guidance and other information specified in ISO/IEC
10 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
<p>An information security policy for cloud computing should be consistent with the organization's acceptable levels of information security risks for their information and other assets.</p> <p>When defining the information security policy for cloud computing, the cloud service customer should take the following into account:</p> <ul style="list-style-type: none">— information stored in the cloud computing environment; which may be subject to access and management by the cloud service provider;— assets maintained in the cloud computing environment, e.g. application programs;— processes run on the cloud service;— users of the cloud service; and,— cloud service customer administrators with elevated privileges.	<p>(no additional implementation guidance)</p>

11

1 **5.1.2 Review of the policies for information security**

- 2 Control 5.1.2 and the associated implementation guidance and other information specified in ISO/IEC
3 27002 apply.

6 Organization of information security

6.1 Internal organization

The objective specified in clause 6.1 of ISO/IEC 27002 applies.

6.1.1 Information security roles and responsibilities

Control 6.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
Different cloud services will have different divisions of responsibilities between the cloud service customer and the cloud service provider. For each type of cloud service used, the division of responsibilities should be defined and documented to ensure the appropriate controls are identified and implemented. Management should assign specific roles and responsibilities across the organization for information security relevant to the use of cloud services.	(no additional implementation guidance)

6.1.2 Segregation of duties

Control 6.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

6.1.3 Contact with authorities

Control 6.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
The cloud service customer should identify the geographical locations where its information is stored, and determine the supervisory authorities and jurisdictions relevant to those locations.	The cloud service provider should inform the cloud service customer of the geographical locations where its information is stored, and the supervisory authorities and jurisdictions relevant to those locations.

6.1.4 Contact with special interest groups

Control 6.1.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

1 **6.1.5 Information security in project management**

2 Control 6.1.5 and the associated implementation guidance and other information specified in ISO/IEC
3 27002 apply.

4 **6.2 Mobile devices and teleworking**

5 The objective specified in clause 6.2 of ISO/IEC 27002 applies.

6 **6.2.1 Mobile device policy**

7 Control 6.2.1 and the associated implementation guidance and other information specified in ISO/IEC
8 27002 apply.

9 **6.2.2 Teleworking**

10 Control 6.2.2 and the associated implementation guidance and other information specified in ISO/IEC
11 27002 apply.

7 Human resource security

7.1 Prior to employment

The objective specified in clause 7.1 of ISO/IEC 27002 applies.

7.1.1 Screening

Control 7.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

7.1.2 Terms and conditions of employment

Control 7.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

7.2 During employment

The objective specified in clause 7.2 of ISO/IEC 27002 applies.

7.2.1 Management responsibilities

Control 7.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

7.2.2 Information security awareness, education and training

Control 7.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
<p>The cloud service customer should ask the cloud service provider for user manuals, precautions and contacts regarding the cloud service.</p> <p>The cloud service customer should add the following items to awareness, education and training programmes for cloud service users, including relevant employees, contractors and third parties:</p> <ul style="list-style-type: none">— standards and procedures for the use of cloud services;— information security risks and their treatment of cloud services; and,— system and network environment risks with the use of cloud services. <p>Information security education, training and awareness about cloud services should be provided to management and the supervising managers, including those of business units. This supports effective co-ordination of information</p>	<p>(no additional implementation guidance)</p>

security activities.	
----------------------	--

1 **7.2.3 Disciplinary process**

2 Control 7.2.3 and the associated implementation guidance and other information specified in ISO/IEC
3 27002 apply.

4 **7.3 Termination and change of employment**

5 The objective specified in clause 7.3 of ISO/IEC 27002 applies.

6 **7.3.1 Termination or change of employment responsibilities**

7 Control 7.3.1 and the associated implementation guidance and other information specified in ISO/IEC
8 27002 apply.

8 Asset management

8.1 Responsibility for assets

The objective specified in clause 8.1 of ISO/IEC 27002 applies.

8.1.1 Inventory of assets

Control 8.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
The inventory of assets should account for those relevant to cloud services and components (e.g., hardware-assisted virtualization, virtualized equipment, virtualized storage, and virtualization software). A process should be established to reconcile the inventory and classification of assets relevant to cloud services and components between the cloud service customer and the cloud service provider.	

Other information for cloud computing

The kinds of cloud service customer assets will very likely vary depending on the category of the cloud service being used. Application software will belong to the cloud service customer in the case of an IaaS service, whereas for a SaaS service, the application software will belong to the cloud service provider.

8.1.2 Ownership of assets

Control 8.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

8.1.3 Acceptable use of assets

Control 8.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

8.1.4 Return of assets

Control 8.1.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
The cloud service customer should ensure that arrangements are made for the return of their assets upon termination of use of a cloud service, or the end of the contract or agreement with the cloud service provider. These arrangements should be documented in an agreement and should be performed in a timely manner. They should include the handling of any backups of assets held by the cloud service provider. In some cases, it may be possible to	(no additional implementation guidance)

ensure that backups are permanently erased. In other cases, it may be necessary to ensure that residual backups are subject to on-going non-disclosure agreements.	
--	--

8.2 Information classification

The objective specified in clause 8.2 of ISO/IEC 27002 applies.

8.2.1 Classification of information

Control 8.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

8.2.2 Labelling of information

Control 8.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

Cloud service customer	Cloud service provider
The cloud service customer should classify information and associated virtualized assets in accordance with the information classification scheme adopted by the cloud service customer. Virtualized assets may include virtualized servers, network equipment, storage, etc.	The cloud service provider should provide the functionality that allows the cloud service customer to label the customers' information and associated virtualized assets. Virtualized assets may include virtualized servers, network equipment, storage, etc.

8.2.3 Handling of assets

Control 8.2.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

8.3 Media handling

The objective specified in clause 8.3 of ISO/IEC 27002 applies.

8.3.1 Management of removable media

Control 8.3.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

8.3.2 Disposal of media

Control 8.3.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

8.3.3 Physical media transfer

Control 8.3.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

9 Access control

9.1 Business requirements of access control

The objective specified in clause 9.1 of ISO/IEC 27002 applies.

9.1.1 Access control policy

Control 9.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

9.1.2 Access to networks and network services

Control 9.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
The network services policy should include network access controls for each cloud service.	The cloud service provider should provide network access controls for each cloud service used by the cloud service customer. The controls should include rules for determining who can have access and the scope of their access.

9.2 User access management

The objective specified in clause 9.2 of ISO/IEC 27002 applies.

9.2.1 User registration and de-registration

Control 9.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

9.2.2 User access provisioning

Control 9.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

Other information for cloud computing

It is strongly recommended that the cloud service provide support for third party Identity and Access Management technologies with respect to their cloud services and the associated administration interfaces. These technologies can enable easier integration and easier user identity administration between the cloud service customer systems and the cloud service and also ease the use of multiple cloud services, supporting such capabilities as Single Sign-On.

9.2.3 Management of privileged access rights

Control 9.2.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
-------------------------------	-------------------------------

The cloud service customer should use strong authentication for authenticating the cloud service customer's administrators.	The cloud service provider should provide strong authentication features for authenticating the cloud service customer's administrators. e.g., multi-factor authentication.
---	---

1

2 Other information for cloud computing

3 Virtualized systems and other assets can be easily deleted or disabled by the operation of the
 4 customer cloud service administrator, e.g., by operation through control panels. Unauthorized
 5 operation can have huge impacts to the availability of the service.

6 **9.2.4 Management of secret authentication information of users**

7 Control 9.2.4 and the associated implementation guidance and other information specified in ISO/IEC
 8 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
The cloud service customer should confirm that the password management process functionality used by the cloud service follows the procedures required by the cloud service customer.	The cloud service provider should provide information on procedures for management of secret authentication information, including procedures for distribution of such information and procedures for user authentication.

9

10 **9.2.5 Review of user access rights**

11 Control 9.2.5 and the associated implementation guidance and other information specified in ISO/IEC
 12 27002 apply.

13 **9.2.6 Removal or adjustment of access rights**

14 Control 9.2.6 and the associated implementation guidance and other information specified in ISO/IEC
 15 27002 apply.

16 **9.3 User responsibilities**

17 The objective specified in clause 9.3 of ISO/IEC 27002 applies.

18 **9.3.1 Use of secret authentication information**

19 Control 9.3.1 and the associated implementation guidance and other information specified in ISO/IEC
 20 27002 apply.

21 **9.4 System and application access control**

22 The objective specified in clause 9.4 of ISO/IEC 27002 applies.

23 **9.4.1 Information access restriction**

24 Control 9.4.1 and the associated implementation guidance and other information specified in ISO/IEC
 25 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
The cloud service customer should ensure that access to information can be restricted in accordance with its access control policy and that such restrictions are realized. (see 13.1.1) This includes access to cloud services, cloud service functions, and cloud service customer's information maintained in the service.	The cloud service provider should provide access controls that allow the cloud service customer to restrict access to cloud services, cloud service functions and cloud service customer's information maintained in the service.

1

2 **9.4.2 Secure log-on procedures**

3 Control 9.4.2 and the associated implementation guidance and other information specified in ISO/IEC
4 27002 apply.

5 **9.4.3 Password management system**

6 Control 9.4.3 and the associated implementation guidance and other information specified in ISO/IEC
7 27002 apply.

8 **9.4.4 Use of privileged utility programs**

9 Control 9.4.4 and the associated implementation guidance and other information specified in ISO/IEC
10 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
<p>The cloud service customer should describe the requirements for any utility programs used within the cloud service environment and ensure that the cloud service provider meets these requirements.</p> <p>The cloud service customer should ensure that no utility programs capable of overriding system and application controls should be run in the cloud environment without permission from the cloud service customer.</p>	(no additional implementation guidance)

11

12 **9.4.5 Access control to program source code**

13 Control 9.4.5 and the associated implementation guidance and other information specified in ISO/IEC
14 27002 apply.

10 Cryptography

10.1 Cryptographic controls

The objective specified in clause 10.1 of ISO/IEC 27002 applies.

10.1.1 Policy on the use of cryptographic controls

Control 10.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
<p>The cloud service customer should consider cryptographic controls that cannot be compromised by the cloud service provider or any other remote party.</p> <p>The cloud service customer should request information from the cloud service provider to confirm that the cryptography and encryption functionalities:</p> <ul style="list-style-type: none"> — meet the requirements of the customer's policy; — are compatible with the cryptographic protection that will be used by the cloud service customer; and, — apply to data being transferred to and from the cloud service, as well as for data stored within the cloud service. 	<p>(no additional implementation guidance)</p>

7

10.1.2 Key management

Control 10.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
<p>The cloud service customer should identify the cryptographic keys it needs to use and manage with a cloud services, and establish procedures for key management.</p> <p>Where the cloud service itself has key management functionality, the cloud service customer should request the following information on the procedures used to manage keys related to cloud service:</p> <ul style="list-style-type: none"> — type of keys; 	<p>The cloud service provider should provide capabilities for the cloud service customer to independently store and manage encryption keys used for protection of any data owned or managed by the cloud service customer.</p> <p>The cloud service provider should provide information on its key management service to the cloud service customer, including but not restricted to:</p> <ul style="list-style-type: none"> — type of keys;

<ul style="list-style-type: none"> — specifications of the key management system, including procedures for each stage of the key life-cycle, i.e. generating, changing or updating, storing, retiring, retrieving, retaining and destroying; and, — recommended key management procedures for use by the customer. <p>The cloud service customer should not permit the cloud service provider to store and manage encryption keys for cryptographic operations that are performed using equipment that is on customer controlled sites, and outside the scope of services provided by cloud service provider. The cloud service customer should employ a separate and distinct service to store and manage these keys.</p>	<ul style="list-style-type: none"> — specifications of the key management system, including procedures for generating, changing or updating, storing, retiring, retrieving, retaining and destroying of keys; and, — recommended key management procedures to be used by the cloud service customer.
--	--

11 Physical and environmental security

11.1 Secure areas

The objective specified in clause 11.1 of ISO/IEC 27002 applies.

11.1.1 Physical security perimeter

Control 11.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

11.1.2 Physical entry controls

Control 11.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

11.1.3 Securing offices, rooms and facilities

Control 11.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

11.1.4 Protecting against external and environmental threats

Control 11.1.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

11.1.5 Working in secure areas

Control 11.1.5 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. .

11.1.6 Delivery and loading areas

Control 11.1.6 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

11.2 Equipment

The objective specified in clause 11.2 of ISO/IEC 27002 applies.

11.2.1 Equipment siting and protection

Control 11.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

11.2.2 Supporting utilities

Control 11.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

11.2.3 Cabling security

Control 11.2.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

1 **11.2.4 Equipment maintenance**

2 Control 11.2.4 and the associated implementation guidance and other information specified in ISO/IEC
3 27002 apply.

4 **11.2.5 Removal of assets**

5 Control 11.2.5 and the associated implementation guidance and other information specified in ISO/IEC
6 27002 apply.

7 **11.2.6 Security of equipment and assets off-premises**

8 Control 11.2.6 and the associated implementation guidance and other information specified in ISO/IEC
9 27002 apply.

10 **11.2.7 Secure disposal or re-use of equipment**

11 Control 11.2.7 and the associated implementation guidance and other information specified in ISO/IEC
12 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
The cloud service customer should ensure that arrangements are made for the secure re-use of resources (equipment, storages, files or memories etc.) upon re-allocation of resources. The arrangements should be covered by a contract or agreement and should be performed in a timely manner.	(no additional implementation guidance)

13

14 **11.2.8 Unattended user equipment**

15 Control 11.2.8 and the associated implementation guidance and other information specified in ISO/IEC
16 27002 apply.

17 **11.2.9 Clear desk and clear screen policy**

18 Control 11.2.9 and the associated implementation guidance and other information specified in ISO/IEC
19 27002 apply.

12 Operations security

12.1 Operational procedures and responsibilities

The objective specified in clause 12.1 of ISO/IEC 27002 applies.

12.1.1 Documented operating procedures

Control 12.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

12.1.2 Change management

Control 12.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
The cloud service customer's change management process should take into account the impact of any changes that may be made by the cloud service provider.	<p>The cloud service provider should provide the cloud service customer with information regarding any changes to a cloud service and the systems on which they run. The following will help the cloud service customer determine the effect the changes may have on information security:</p> <ul style="list-style-type: none"> — categories of significant changes; — planned date and time of the changes; — technical description of the changes to the cloud service and underlying systems; and, — start and completion of the changes. <p>When a cloud service provider offers a cloud service that depends on a peer cloud service provider, then the cloud service provider may need to inform the cloud service customer of changes caused by the peer cloud service provider.</p>

10

12.1.3 Capacity management

Control 12.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
------------------------	------------------------

<p>The cloud service customer should ensure that the agreed to capacity provided by the cloud service is sufficient to meet the cloud service customer's requirements.</p> <p>The use of cloud services should be monitored, and future capacity needs should be forecasted, in order to make efficient use of the cloud services over time.</p>	<p>The cloud service provider should monitor the total capacity of logical and physical computing resources to prevent severe information security incidents caused by resource shortages.</p>
--	--

Other information for cloud computing

The cloud service customer should consider the following for capacity management, if available from the cloud service provider:

c) system environment

- data storage;
- capacity of network and network equipment including the virtual network in the cloud service environment (e.g., bandwidth, maximum number of network sessions);
- agreed or expected system performance;
- lead time to have additional capacity or system performance, and minimum unit of the addition;
- maximum capacity and system performance;
- redundancy and diversity of systems;
- redundancy and diversity of access networks.

d) statistics on system resource usage

- statistics in a given time period;
- maximum system resource usage.

The total volume of logical capacity can never exceed the total volume of physical capacity. If volume requirements exceeded the total volume of physical capacity, it may cause severe incidents. For this reason, monitoring the total volume of logical computing resource and keeping a certain volume of extra resources available is required to prevent incidents caused by lack of resource.

12.1.4 Separation of development, testing and operational environments

Control 12.1.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

12.2 Protection from malware

The objective specified in clause 12.2 of ISO/IEC 27002 applies.

1 **12.2.1 Controls against malware**

2 Control 12.2.1 and the associated implementation guidance and other information specified in ISO/IEC
3 27002 apply.

4 **12.3 Backup**

5 The objective specified in clause 12.3 of ISO/IEC 27002 applies.

6 **12.3.1 Information backup**

7 Control 12.3.1 and the associated implementation guidance and other information specified in ISO/IEC
8 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
The cloud service customer should request the specifications of the backup capabilities from the cloud service provider and should verify that they meet the backup requirements of the cloud service customer.	<p>The cloud service provider should provide the specifications of its backup capabilities to the cloud service customer. The specifications should include the following information, (as appropriate):</p> <ul style="list-style-type: none"> — scope and schedule of backups; — backup methods and data formats (including encryption, if relevant); — retention periods for backup data; — procedures for verifying integrity of backup data; — procedure and timescales involved in restoring data from backup; and, — procedure to test the backup capabilities.

9

10 **12.4 Logging and monitoring**

11 The objective specified in clause 12.4 of ISO/IEC 27002 applies.

12 **12.4.1 Event logging**

13 Control 12.4.1 and the associated implementation guidance and other information specified in ISO/IEC
14 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
The cloud service customer should request from the cloud service provider the specifications of the logging information produced and retained by the cloud service provider, in relation to a cloud service and its associated resources:	The cloud service provider should provide specifications to the cloud service customer about the logging information produced and retained in relation to a cloud service and its associated resources:

<ul style="list-style-type: none"> — the types of log records; — the retention periods which apply to each type of record; and, — the rights the customer has to inspect log records and the procedures for inspecting log records. <p>For logging information that is produced by software controlled by the cloud service customer running in a cloud service (e.g. IaaS or PaaS service), the customer should ensure that logging information is written to permanent, non-volatile storage that can be accessed by the customer at a later point in time.</p>	<ul style="list-style-type: none"> — the types of log records; — the retention periods which apply to each type of record; and, — the rights the customer has to inspect log records and the procedures for inspecting log records. <p>Where a cloud service customer is permitted to access log records controlled by the cloud service provider, the provider should ensure that the customer could only access records that relate to that customer's activities, and cannot access any log records which relate to the activities of other cloud service customers.</p>
--	--

Other information for cloud computing

Some key aspects about logging in the cloud service environment are that:

- logging occurs on the cloud service provider's systems, whether the software doing the logging belongs to the provider or belongs to the customer;
- there are logs that are under the control of the provider. The customer needs to know what is in these logs and whether the customer can access information in those logs and if so, how access is provided; and,
- for logs generated by cloud customer software, there will be a need for the customer to get and retain the information in these logs in a reliable way. The challenge is to store the logs in permanent storage because, in virtual environments, software instances are run automatically in volatile environments (e.g., virtual machines) that are destroyed when the software instance is stopped.

12.4.2 Protection of log information

Control 12.4.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

12.4.3 Administrator and operator logs

Control 12.4.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

12.4.4 Clock synchronisation

Control 12.4.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

12.5 Control of operational software

The objective specified in clause 12.5 of ISO/IEC 27002 applies.

12.5.1 Installation of software on operational systems

Control 12.5.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

12.6 Technical vulnerability management

The objective specified in clause 12.6 of ISO/IEC 27002 applies.

12.6.1 Management of technical vulnerabilities

Control 12.6.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
<p>The cloud service customer should request information from the cloud service provider about technical vulnerability management as it applies to the cloud service and the resources it uses.</p> <p>The information provided should describe the provider's approach to the points made in the guidance contained in clause 12.6.1 of ISO 27002.</p>	<p>The cloud service provider should provide information to the cloud service customers about technical vulnerability management as it applies to the cloud service and the resources it uses.</p> <p>The information provided should describe the provider's approach to the points made in the guidance contained in clause 12.6.1 of ISO 27002.</p>

12.6.2 Restrictions on software installation

Control 12.6.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
<p>Installing commercial licensed software into a cloud service could cause a breach of the license terms for the software. The cloud service customer should have a procedure for checking the license terms before permitting any licensed software to be installed into a cloud service. Particular attention should be paid to cases where the cloud service is elastic and scalable and where the software might be run on more systems or on more processors than the license permits.</p>	<p>(no additional implementation guidance)</p>

12.7 Information systems audit considerations

The objective specified in clause 12.7 of ISO/IEC 27002 applies.

12.7.1 Information systems audit controls

Control 12.7.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

13 Communications security**13.1 Network security management**

The objective specified in clause 13.1 of ISO/IEC 27002 applies.

13.1.1 Network controls

Control 13.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

13.1.2 Security of network services

Control 13.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

13.1.3 Segregation in networks

Control 13.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
The cloud service customer should request information from the cloud service provider on the logical segregation of network access in multi-tenant environments, based on separate network domains.	<p>The cloud service provider should enforce logical segregation of network access for the following:</p> <ul style="list-style-type: none"> — separation of multi-tenant cloud service customer environments; and — separation of cloud service provider internal administration from the customer's cloud computing environment or any other unauthorized users.

Other information for cloud computing

Examples of when segregate networks may be required include:

- competitors within the same industry co-existing within same cloud environment; and,
- regulatory requirements dictating the segregation/isolation of network traffic

13.2 Information transfer

The objective specified in clause 13.2 of ISO/IEC 27002 applies.

13.2.1 Information transfer policies and procedures

Control 13.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

13.2.2 Agreements on information transfer

Control 13.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

1 **13.2.3 Electronic messaging**

2 Control 13.2.3 and the associated implementation guidance and other information specified in ISO/IEC
3 27002 apply.

4 **13.2.4 Confidentiality or non-disclosure agreements**

5 Control 13.2.4 and the associated implementation guidance and other information specified in ISO/IEC
6 27002 apply.

7

14 System acquisition, development and maintenance**14.1 Security requirements of information systems**

The objective specified in clause 14.1 of ISO/IEC 27002 applies.

14.1.1 Security requirements analysis and specification

Control 14.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
<p>The cloud service customer should determine their security requirements for the cloud service and then evaluate whether or not services offered by a cloud service provider can meet these requirements.</p> <p>The cloud service customer should obtain from the cloud service provider a description of the information security controls implemented by the provider.</p> <p>The cloud service customer should include the security requirements of cloud services in their analysis.</p>	(no additional implementation guidance)

14.1.2 Securing applications services on public networks

Control 14.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

14.1.3 Protecting application services transactions

Control 14.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

14.2 Security in development and support processes

The objective specified in clause 14.2 of ISO/IEC 27002 applies.

14.2.1 Secure development policy

Control 14.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

14.2.2 System change control procedures

Control 14.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

1 **14.2.3 Technical review of applications after operating platform changes**

2 Control 14.2.3 and the associated implementation guidance and other information specified in ISO/IEC
3 27002 apply.

4 **14.2.4 Restrictions on changes to software packages**

5 Control 14.2.4 and the associated implementation guidance and other information specified in ISO/IEC
6 27002 apply.

7 **14.2.5 Secure system engineering principles**

8 Control 14.2.5 and the associated implementation guidance and other information specified in ISO/IEC
9 27002 apply.

10 **14.2.6 Secure development environment**

11 Control 14.2.6 and the associated implementation guidance and other information specified in ISO/IEC
12 27002 apply.

13 **14.2.7 Outsourced development**

14 Control 14.2.7 and the associated implementation guidance and other information specified in ISO/IEC
15 27002 apply.

16 **14.2.8 System security testing**

17 Control 14.2.8 and the associated implementation guidance and other information specified in ISO/IEC
18 27002 apply.

19 **14.2.9 System acceptance testing**

20 Control 14.2.9 and the associated implementation guidance and other information specified in ISO/IEC
21 27002 apply.

22 Other information for cloud computing

23 In cloud computing, guidance for system acceptance testing applies to the use of a cloud service by
24 the cloud service customer.

25 **14.3 Test data**

26 The objective specified in clause 14.3 of ISO/IEC 27002 applies.

27 **14.3.1 Protection of test data**

28 Control 14.3.1 and the associated implementation guidance and other information specified in ISO/IEC
29 27002 apply.

1 15 Supplier relationships

2 15.1 Security in supplier relationship

3 The objective specified in clause 15.1 of ISO/IEC 27002 applies.

4 15.1.1 Information security policy for supplier relationships

5 Control 15.1.1 and the associated implementation guidance and other information specified in ISO/IEC
6 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
The cloud service customer should include the cloud service provider as a type of supplier in their information security policy for supplier relationships. This will help to mitigate risks associated with the cloud service provider's access to the cloud service customer's information.	The cloud service provider should ensure that the security controls of a cloud service it gets from a peer cloud service provider meet or exceed the security requirements of their cloud service customer.

7

8 15.1.2 Addressing security within supplier agreements

9 Control 15.1.2 and the associated implementation guidance and other information specified in ISO/IEC
10 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
<p>The cloud service customer should confirm its information security roles and responsibilities in the service agreement. These can include the following processes:</p> <ul style="list-style-type: none"> — malware protection; — backup; — cryptographic control; — vulnerability management; — incident management; — collection of evidence; and, — technical compliance. 	<p>The cloud service provider should provide service specifications for security controls that will be provided to support the candidate cloud service customer. This will help the cloud service customer evaluate the controls against its information security policies on supplier relationships and the use of cloud computing.</p> <p>Roles and responsibilities of the cloud service provider should be considered for the following processes:</p> <ul style="list-style-type: none"> — malware protection; — backup; — cryptographic control; — vulnerability management; — incident management; — collection of evidence; and,

	<p>— technical compliance.</p> <p>When the cloud service provider provides cloud services based on a supply chain, the cloud service provider should provide risk management objectives to suppliers and request each of the suppliers to perform risk management activities to achieve the objectives.</p>
--	---

1

2 **15.1.3 Information and communication technology supply chain**

3 Control 15.1.3 and the associated implementation guidance and other information specified in ISO/IEC
4 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
(no additional implementation guidance)	If a cloud service provider is a cloud service customer of other services, the cloud service provider should pass through the service levels of its suppliers. The cloud service provider should ensure that the service levels guaranteed to its cloud service customers do not interfere with lower service levels of its own suppliers.

5

6 **15.2 Supplier service delivery management**

7 The objective specified in clause 15.2 of ISO/IEC 27002 applies.

8 **15.2.1 Monitoring and review of supplier services**

9 Control 15.2.1 and the associated implementation guidance and other information specified in ISO/IEC
10 27002 apply.

11 **15.2.2 Managing changes to supplier services**

12 Control 15.2.2 and the associated implementation guidance and other information specified in ISO/IEC
13 27002 apply.

16 Information security incident management

16.1 Management of information security incidents and improvements

The objective specified in clause 16.1 of ISO/IEC 27002 applies.

16.1.1 Responsibilities and procedures

Control 16.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
The cloud service customer and cloud service provider should mutually reconcile responsibilities and processes for managing information security incidents to ensure alignment such that information security incidents are assessed and reported in a timely manner.	

16.1.2 Reporting information security events

Control 16.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud Service Customer	Cloud Service Provider
<p>The cloud service customer should get information from the cloud service provider about:</p> <ul style="list-style-type: none"> — the mechanism by which the cloud service customer can report information security events it has discovered to the cloud service provider; — the mechanism by which the cloud service provider can report security events it has discovered to the cloud service customer; and, — the mechanism by which the cloud service customer can track what is happening in relation to a reported information security event. 	<p>The cloud service provider should provide mechanisms for:</p> <ul style="list-style-type: none"> — a cloud service customer to report an information security event to the provider; — the cloud service provider to report an information security event to a cloud service customer; and, — the customer to track what is happening in relation to a reported information security event.

Other information for cloud computing

Given that an information security event may be discovered either by the cloud service customer or by the cloud service provider, the main additional responsibility relating to cloud computing is that the party discovering the event should have procedures to report the event to the other party immediately.

16.1.3 Reporting information security weaknesses

Control 16.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

1 **16.1.4 Assessment of and decision on information security events**

2 Control 16.1.4 and the associated implementation guidance and other information specified in ISO/IEC
3 27002 apply.

4 **16.1.5 Response to information security incidents**

5 Control 16.1.5 and the associated implementation guidance and other information specified in ISO/IEC
6 27002 apply.

7 **16.1.6 Learning from information security incidents**

8 Control 16.1.6 and the associated implementation guidance and other information specified in ISO/IEC
9 27002 apply.

10 **16.1.7 Collection of evidence**

11 Control 16.1.7 and the associated implementation guidance and other information specified in ISO/IEC
12 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
The cloud service customer and the cloud service provider should mutually reconcile and agree on the policies and processes to respond to requests for evidence of information within the cloud computing environment. Specifically, restrictions on acquisition of evidence should be defined and mutually agree to between the cloud service customer and the cloud service provider.	

13

1 **17 Information security aspects of business continuity management**

2 **17.1 Information security continuity**

3 The objective specified in clause 17.1 of ISO/IEC 27002 applies.

4 **17.1.1 Planning information security continuity**

5 Control 17.1.1 and the associated implementation guidance and other information specified in ISO/IEC
6 27002 apply.

7 **17.1.2 Implementing information security continuity**

8 Control 17.1.2 and the associated implementation guidance and other information specified in ISO/IEC
9 27002 apply.

10 **17.1.3 Verify, review and evaluate information security continuity**

11 Control 17.1.3 and the associated implementation guidance and other information specified in ISO/IEC
12 27002 apply.

13 **17.2 Redundancies**

14 The objective specified in clause 17.2 of ISO/IEC 27002 applies.

15 **17.2.1 Availability of information processing facilities**

16 Control 17.2.1 and the associated implementation guidance and other information specified in ISO/IEC
17 27002 apply.

18 Compliance

18.1 Compliance with legal and contractual requirements

The objective specified in clause 18.1 of ISO/IEC 27002 applies.

18.1.1 Identification of applicable legislation and contractual requirements

Control 18.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
<p>The cloud service customer should identify relevant legal, regulatory and contractual requirements and have ensured that they are fulfilled while using the cloud service.</p> <p>The cloud service customer should have evidence on the cloud service provider's compliance, with relevant standards required for the cloud service customer's business.</p>	<p>The cloud service provider should assist the cloud service customer in its efforts to identify applicable laws and regulations in the jurisdictions where the cloud services are produced and/or provided.</p> <p>The cloud service provider should identify the coverage and limitations in meeting the legal and regulatory requirements of its services, and provide the information to the cloud service customer when required. For example, use of encryption and protection of PII.</p> <p>The cloud service provider should provide the cloud service customer with evidence of compliance to standards required for the cloud service customer's business.</p>

Other information for cloud computing

Applicable legal and regulatory requirements should be carefully identified in the use and provision of cloud services which have globally distributed storage and communication capabilities. Encryption of information and protection of PII are the examples which legal and regulatory requirements can vary depending on the jurisdictions for.

18.1.2 Intellectual property rights (IPR)

Control 18.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

18.1.3 Protection of records

Control 18.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

18.1.4 Privacy and protection of personally identifiable information

Control 18.1.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. ISO/IEC 27018 Code of practice for data protection controls for public computing services can offer additional information on this topic.

18.1.5 Regulation of cryptographic controls

Control 18.1.5 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
The cloud service customer should define the cryptographic requirements associate with regulatory compliance and verify that the cloud service provider meets those requirements.	(no additional implementation guidance)

18.2 Information security reviews

The objective specified in clause 18.2 of ISO/IEC 27002 applies.

18.2.1 Independent review of information security

Control 18.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

18.2.2 Compliance with security policies and standards

Control 18.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

18.2.3 Technical compliance review

Control 18.2.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

Annex A

Cloud Service Extended Control Set

(normative)

This Annex provides additional objectives and controls with implementation guidance, as a cloud service extended control set. ISO/IEC 27002 control objectives related to these controls are not repeated. It is recommended that any organization implementing these controls in the context of an ISMS, which is intended to be conformant to ISO/IEC 27001, extend their SOA (statement of applicability) by the inclusion of the controls stated in this Annex.

CLD.6.3 Relationship between cloud service customer and cloud service provider

Objective; To establish and maintain a collaborative relationship between the cloud service customer and the cloud service provider for information security management.

CLD.6.3.1 Demarcation of responsibility

Control

The demarcation between the responsibilities of the cloud service customer and cloud service provider should be defined and documented.

Implementation guidance

Cloud service customer	Cloud service provider
<p>The cloud service customer should identify and manage the support contact and the customer contact of the cloud service provider.</p> <p>The cloud service customer should review the proposed demarcation of information security responsibilities and confirm if it can accept its responsibilities. Responsibilities of both parties should be stated in the agreement.</p>	<p>The cloud service provider should define and document the demarcation of responsibilities of cloud service customer, cloud service provider and its suppliers. When agreed, the cloud service provider should define and document sub-contractor responsibilities.</p>

Other information for cloud computing

Ambiguity in roles and in the definition of responsibilities related to issues such as data ownership, access control, and infrastructure maintenance, may give rise to business or legal disputes, especially when dealing with third parties, or when the cloud service provider is also a cloud service customer or cloud service sub-contractor.

Data and files generated by the system or application of the cloud service during its operation can be critical for secure operation, recovery and continuity of the service. Owners of these assets, and the responsibilities of associated operations, should be defined and documented. For example, backup and recovery operations.

1 **CLD.9.5 Access control of cloud service customer's data in shared virtual environment**

Objective: To ensure information security in virtual environment on shared cloud computing.

2 **CLD.9.5.1 Segregation in virtual computing environments**

3 Control

4 Cloud service customer's virtual environment on a cloud service should be protected from other cloud
5 service customers and unauthorized users.

6 Implementation guidance

Cloud service customer	Cloud service provider
(no additional implementation guidance)	<p>The cloud service provider should enforce logical segregation of virtualized application, operating system , storage, and network for the following:</p> <ul style="list-style-type: none"> — separation cloud service customers in multi-tenant environments; and, — separation of the cloud service provider's internal administration. <p>Where the cloud service involves multi-tenancy, the cloud service provider should implement information security controls to ensure isolation of different tenants.</p> <p>The cloud service provider should consider the risks associated with running customer-supplied software within the cloud services offered by the provider.</p>

7

8 Other information for cloud computing

9 When a virtual environment is provided by a software virtualization function (e.g. a virtual operating
10 system), network and storage configurations can be virtualized, and segregation of physical networks
11 can be made invalid. Segregation of cloud service customers in software virtualized environments
12 should be designed and implemented using segregation functions of the software.

13 When a cloud service customer's information is stored in a physically shared storage area with
14 "meta-data table" of the cloud service, segregation of information from other cloud service customers
15 can be implemented by access control on the "meta-data table".

CLD.12.1 Operations security

CLD.12.1.2 Administrator's operational security

Control

Procedures for critical operations of cloud computing environment should be defined, documented and monitored.

Implementation guidance

Cloud service customer	Cloud service provider
<p>The cloud service customer should document procedures for critical operations where a failure can cause unrecoverable damage to assets in the cloud computing environment. These operations should be performed monitored and checked by a supervisor.</p> <p>Examples of the critical operations are:</p> <ul style="list-style-type: none">— installation, changes, and deletion of virtualized devices such as servers, networks and storage;— termination procedures for cloud service usage: and,— backup and restoration.	<p>The cloud service provider should introduce processes and documentation for critical operations where failure can cause unrecoverable damage to assets in cloud computing environment.</p> <p>The following should be considered for inclusion in the process:</p> <ul style="list-style-type: none">— interactive step-by-step operations;— dual operation; and,— monitoring and checking by a supervisor. <p>Examples of the operations which can cause significant damages to the cloud computing environment are:</p> <ul style="list-style-type: none">— installation, changes and deletion of virtualized devices such as servers, networks, storages;— discontinuation of cloud services; and,— backup and restoration.

Other information for cloud computing:

Cloud computing has the benefit of "rapid provisioning and administration of on-demand self-service". This is often carried out by the administrators from the cloud service customer and the cloud service provider. Because human intervention to these critical operations can cause serious information security incidents, controls to safeguard the operations should be defined and implemented. Examples of serious incidents include erasing or shutting down a large number of virtual servers, or destroying virtual assets.

CLD.12.4 Logging and monitoring

The objective specified in sub clause 12.4 of ISO/IEC 27002 applies.

1 CLD.12.4.3 Administrator and operator logs

2 Control

3 The operation log of cloud service customer's privileged use should be acquired and stored to clarify
4 responsibility boundaries.

5 Implementation guidance

Cloud service customer	Cloud service provider
(no additional implementation guidance)	If a privileged operation in the cloud computing environment was delegated to the cloud service customer, then the operation logs by both the cloud service provider and the cloud service customer should be acquired and stored to clarify responsibility boundaries.

6

7 CLD.12.4.5 Monitoring of Cloud Services

8 Control

9 The cloud service customer should have the capability to monitor the operation of the cloud services
10 which the customer uses.

11 Implementation guidance

Cloud service customer	Cloud service provider
The cloud service customer should request documentation from the cloud service provider of the monitoring facilities available in respect of each cloud service which.	<p>The cloud service provider should provide facilities to the cloud service customer which enable the cloud service customer to monitor the operation and use of cloud services. The monitoring facilities should be secured and should only provide access to information about the customer's own cloud service instances.</p> <p>The cloud service provider should provide documentation of the monitoring facilities to the cloud service customer.</p> <p>Monitoring should provide data equivalent to the event logs described in clause 12.4.1 and also should include data relating to terms in the SLA and the metrics which relate to each identified service level target.</p>

12

13 CLD.13 Communications security

14 CLD.13.1 Network security management

15 The objective specified in sub clause 13.1 of ISO/IEC 27002 applies.

CLD.13.1.4 Cooperation of configurations between virtual and physical network

Control

Upon configuration of virtual network, consistency of configurations between virtual and physical network should be verified based on the organization's network security policy.

Implementation guidance

Cloud service customer	Cloud service provider
(no additional implementation guidance)	The cloud service provider should ensure that there is a policy relating to the configuration of the virtual network that is consistent with the security policy that applies to the physical network. The cloud service provider should ensure that the virtual security configuration matches the configuration policy, whatever the means used to create the configuration.

Other information for cloud computing

In cloud computing environment built on virtualized technology, virtual network is configured on virtual infrastructure on physical network. In such environment, inconsistency of network policies could cause system outage and/or access control violation.

Annex B

References on information security risk related cloud computing (informative)

Proper use of the information security controls provided by this Recommendation | International Standard relies on an information security risk assessment and an understanding of information security risk treatment. Although these are important subject, they are not within the scope of this document. Annex B provides references on risk assessment and risk treatment approaches.

Editor's note: NBs and liaisons are requested to provide references information on information references.

For example,

(1) ITU-T SG17

(a) Title: Security framework for cloud computing (ITU-T X.1600)

(b) Approach: Security threats, Security challenges, Security capabilities

(2) NIST

(a) Title: Risk Management Guide for Information Technology Systems (NIST SP 800-30)

(b) Approach: Risk management guide for Computer Security

Bibliography

- 2 [1] ISO/IEC16680:2012, The Open Group Service Integration Maturity Model (OSIMM)
- 3 [2] ISO/IEC 17788:201x, Information technology — Distributed application platforms and services
- 4 — Cloud computing — Overview and Vocabulary
- 5 [3] ISO/IEC 17789:201x, Information technology — Distributed Application Platforms and Services
- 6 — Cloud Computing — Reference Architecture
- 7 [4] ISO/IEC 18028-1:2006, Information technology - Security techniques - IT network security -
- 8 Part 1: Network security management.
- 9 [5] ISO/IEC 18028-2:2006, Information technology - Security techniques - IT network security -
- 10 Part 2: Network security architecture.
- 11 [6] ISO/IEC 18028-3:2005, Information technology - Security techniques - IT network security -
- 12 Part 3: Securing communications between networks using security gateways.
- 13 [7] ISO/IEC 18028-4:2005, Information technology - Security techniques - IT network security -
- 14 Part 4: Securing remote access.
- 15 [8] ISO/IEC 18028-5:2006, Information technology - Security techniques - IT network security -
- 16 Part 5: Securing communications across networks using virtual private networks
- 17 [9] ISO/IEC 18043:2006, Information technology - Security techniques - Selection, deployment
- 18 and operations of intrusion detection systems.
- 19 [10] ISO/IEC TR 18044:2004, Information technology - Security techniques - Information security
- 20 incident management.
- 21 [11] ITU-T Recommendation X.805 (2003), Security architecture for systems providing end-to-end
- 22 communications.
- 23 [12] U.S. CIO Council, Proposed Security Assessment & Authorization for U.S. Government Cloud
- 24 Computing
- 25 [13] NIST, SP800-144 Guidelines on Security and Privacy in Public Cloud Computing
- 26 [14] NIST, SP800-145 The NIST Definition of Cloud Computing (Draft)
- 27 [15] NIST, Effectively and Securely Using the Cloud Computing Paradigm
- 28 [16] ENISA, Cloud Computing Benefits, risks and recommendations for information security
- 29 [17] ENISA, Cloud Computing Information Assurance Framework
- 30 [18] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing
- 31 V2.1
- 32 [19] Cloud Security Alliance, Top Threats to Cloud Computing V1.0
- 33 [20] Cloud Security Alliance, Domain 12: Guidance for Identity & Access Management V2.1

- 1 [21] Cloud Security Alliance, CSA Cloud Controls Matrix V1.1
- 2 [22] ISACA, Cloud Computing: Business Benefits With Security, Governance and Assurance
- 3 Perspectives
- 4 [23] ISACA, Cloud Computing Management Audit/Assurance Program