



ISO/IEC JTC 1/SC 27 **N11916**

ISO/IEC JTC 1/SC 27/WG 1 **N11916**

REPLACES: N11122

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC. TYPE: Working Draft text

TITLE: Text for ISO/IEC 4th WD 27017 – Information technology — Security techniques — Code of practice for information security controls for cloud computing services based on ISO/IEC 27002*

SOURCE: Project co-editors (S. Yamasaki, M. Pohlman, K. Nakao)

DATE: 2012-12-17

PROJECT: 1.27.91 (27017)

STATUS: In accordance with Resolution 8 (contained in SC 27 N11900) of the 45th SC 27/WG 1 meeting in Rome (Italy) 26th October 2012, this document is circulated for STUDY AND COMMENT.

National Bodies and liaison organizations of SC 27 are requested to send their comments / contributions on the above-mentioned Working Draft by **2013-02-25**.

PLEASE submit your comments / contributions on the hereby attached document via the SC 27 e-balloting website at: <http://isotc.iso.org/livelink/livelink/open/jtc1sc27>

PLEASE NOTE: For comments please use THE SC 27 TEMPLATE separately attached to this document.

ACTION ID: COMM

DUE DATE: 2013-02-25

DISTRIBUTION: P-, O- and L-Members
W. Fumy, SC 27 Chairman
M. De Soete, SC 27 Vice Chair
E. J. Humphreys, T. Chikazawa, M. Bañón, J. Amsenga, K. Rannenberg, WG-Convenors

MEDIUM: <http://isotc.iso.org/livelink/livelink/open/jtc1sc27>

NO. OF PAGES: 1 + 97

* Title change subject to JTC 1 endorsement

Secretariat ISO/IEC JTC 1/SC 27 –
DIN Deutsches Institut für Normung e. V., Am DIN-Platz, Burggrafenstr. 6, D-10787 [D-10772 postal] Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-4-2652; E-mail: krystyna.passia@din.de;
[HTTP://www.jtc1sc27.din.de/en](http://www.jtc1sc27.din.de/en)

**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:

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

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

Violators may be prosecuted.

Editor's notes

The following notes are summarizing the items which support NBs and liaisons to create comments and contributions on the revised texts based on discussions and resolutions during Rome 27017 editing session.

I. Important information

1. Information regarding the revised texts

- 1) The revised texts reflect Disposition of comments (N11915) and Meeting Report of 27017 editing session (N12017) based on structure of DIS 27002.
- 2) The revised texts are structured based on DIS 27002 (N11907). The following controls of 27002 CD1 are removed from DIS 27002. Therefore, editors evaluated that the cloud specific implementation guidance of these controls of WD3 27017 is integrated to the controls of WD4 27017 as follows.
 - a) 6.1.2 of WD3 27017 is integrated to none.
 - b) 8.2.3 of WD3 27017 is integrated to 7.2.2 of WD4 27017.
 - c) 11.8.4 of WD3 27017 is integrated to 12.4.1 (Event logging).
 - d) 14.4.2 of WD3 27017 is integrated to 14.2.2 (Change control procedures).
 - e) 16.1.3 and 16.1.5 of WD3 27017 is integrated to 17.1.3 (Verify, review and evaluate information security continuity).
 - f) 16.1.4 of WD3 27017 is integrated to none.
 - g) 17.1.5 of WD3 27017 is integrated to 8.1.3 of WD4 27017.
- 3) The following two controls of DIS 27002 are newly added. Therefore, editors evaluated that the following two controls of WD4 27017 do not have the cloud specific implementation guidance of WD3 27017.
 - a) 12.6.2 of WD4 27017 does not have implementation guidance.
 - b) 14.2.8 of WD4 27017 does not have implementation guidance.
- 4) The revised ISO/IEC CD17788 (N11781) has been circulated on 18th November 2012, for CD balloting by cooperation with SC38 and ITU-T. In this standard, cloud consumer and cloud provider are changed to cloud service customer or cloud service user, and cloud service provider. However, editors decided that it is postponed until the next meeting to change cloud consumer and cloud provider to the new terms and definitions, because ISO/IEC 17788 is possibly still changing.

2. Editors work items approved at Rome 27017 editing session in order to proceed editor's work based on ISO/IEC 27017 DoC (SC 27 N11915)

- 1) To apply DoC based on the resolutions (Accepted in principle, Accepted with mods, Accepted)
- 2) To merge and delete the duplicated parts based on DoC
- 3) To change format based on the agreed format based on DoC
- 4) Editors request to NBs and liaisons to provide comments and contributions based on revised texts applied by DoC.

II. Information for NBs and liaisons to work on comments and contributions

1. 27017 revised texts (SC 27 N11916) marked by Editors to identify the following items.

- 1) All modifications and additions to revised 27002 original texts are highlighted as follows.

- a) in BLACK: revised ISO/IEC 27002 original text (SC 27 N11907)

- b) in BLUE:

- ISO/IEC 27017 (SC 27 N10029) original NWIP (WD1)
- ISO/IEC 27017 (SC 27 N10029) cloud specific + WD1 DoC (SC 27 N10593) applied texts (SC 27 N10594:WD2)
- ISO/IEC 27017 (SC 27 N10594) cloud specific + WD2 DoC (SC 27 N11121) applied texts (SC 27 N11122:WD3)
- ISO/IEC 27017 (SC27 N11122) cloud specific + WD3 DoC (SC27N11915) applied texts (SC27 N11916:WD4)

thus these texts have been addressed at Nairobi, Stockholm and Rome meeting.

- 2) The comment and its comment number of DoC are placed in [WD1:xxxx], [WD2:xxxx] and [xxxx] instead of [WD3:xxxx] square brackets.

2. NBs and liaisons are kindly requested to provide comments and contributions mainly regarding the following areas.

- 1) To confirm whether the cloud specific implementation guidance of the WD3 27017 controls is integrated to the controls of WD4 27017 appropriately or not, especially regarding the cloud specific implementation guidance of the removed controls in DIS 27002 and the newly additional controls in DIS27002 (See I-1-2) and 3))
- 2) To confirm whether the applied format for each control is appropriate or not among three types of new table format, for example type 1, type 2 or type 3 (See Clause 4.1) .
- 3) Regarding the texts in Annex A of 27017, to apply either case of the following two cases. This decision has been postponed to the next meeting according to the resolution of Rome 27017 editing meeting. For more details, see Major issue 11 of 27017 meeting report (N12017).
 - a) Case1: To move the regarding cloud specific implementation guidance to the appropriate control of WD4 27017 main body
 - b) Case2: To create “new” additional cloud specific control objective and controls, and put the regarding cloud specific implementation guidance into the regarding “new” additional cloud specific controls
- 4) For US NB, to provide US NB contributions for comments in Rome editing meeting such as US23, US24, US25, US26, US27, US28, US29, US33, US34, US36, US43, US47, US48, US50, US54, US55. In case of no existing implementation guidance for regarding control, editors put table in the regarding control.
- 5) Other items specified as “Editor’s note” in main body of revised 27017 (See more details in SC 27 N11122)
 - a) Regarding clause 4.2, to provide the texts which describes relationships between ISO/IEC 27017 and ISO/IEC 27036. [US3]

- b) Regarding normative reference, to respond on whether ISO/IEC 17788 and ISO/IEC 17789 are normative reference or not. This is postponed from Rome meeting to the next meeting.
- c) NBs and liaisons are requested to provide contributions on Annex B, Annex C and Annex D.

3. Editors actions at Sophia Antipolis meeting

The development schedule of this standard was proposed as Technical Specification (TS) at NWIP stage. Therefore, its target date is planned as October 2013. However, the development schedule of this standard needs to be changed because of the following reasons. As a result, editors will propose development schedule extension at Sophia Antipolis meeting. NBs and liaisons are requested to provide the comments on this subject such as the new target date.

- a) Document type change from TS to IS (Resolution 15 of WG1 Rome meeting)
- b) Collaborative work and collaborative document with ITU-T
- c) Stability of SC38 documents such as ISO/IEC 17788 and 17789 as prerequisite standards

Contents

Foreword	xiv
0 Introduction	xv
0.1 Overview	xv
0.2 Needs	xv
0.3 Objectives	xv
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Overview	3
4.1 Structure of this Guidance	3
4.2 Relations with the other standards	5
4.3 Models	5
4.3.1 General	5
4.3.2 Service model	5
4.3.3 Deployment model	5
4.3.4 Relations between cloud consumer and cloud provider	5
4.4 Assessing security risks in cloud service	5
5 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	7
6 Organisation of information security	8
6.1 Internal organisation	8
6.1.1 Information security roles and responsibilities	8
6.1.2 Contact with authorities	8
6.1.3 Contact with special interest groups	9
6.1.4 Information security in project management	9
6.1.5 Segregation of duties	9
6.2 Mobile devices and teleworking	9
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.....	14
8.2	Information classification.....	14
8.2.1	Classification of information.....	14
8.2.2	Labeling of information	14
8.2.3	Handling of assets	15
8.2.4	Return of assets	15
8.3	Media handling.....	15
8.3.1	Management of removable media.....	16
8.3.2	Disposal of media.....	16
8.3.3	Physical media transfer	16
9	Access control	17
9.1	Business requirements of access control.....	17
9.1.1	Access control policy	17
9.1.2	Policy on the use of network services	17
9.2	User access management.....	18
9.2.1	User registration and de-registration.....	18
9.2.2	Privilege management.....	18
9.2.3	Management of secret authentication information of users	19
9.2.4	Review of user access rights	20
9.2.5	Removal or adjustment of access rights.....	20
9.3	User responsibilities	21
9.3.1	Use of secret authentication information	21
9.4	System and application access control.....	21
9.4.1	Information access restriction	21
9.4.2	Secure log-on procedures.....	21
9.4.3	Password management system.....	22

9.4.4	Use of privileged utility programs	22
9.4.5	Access control to program source code	22
10	Cryptography	23
10.1	Cryptographic controls.....	23
10.1.1	Policy on the use of cryptographic controls.....	23
10.1.2	Key management	23
11	Physical and environmental security	25
11.1	Secure areas	25
11.1.1	Physical security perimeter	25
11.1.2	Physical entry controls	25
11.1.3	Securing office, room and facilities	25
11.1.4	Protecting against external and environmental threats	25
11.1.5	Working in secure areas	25
11.1.6	Delivery and loading areas.....	25
11.2	Equipment.....	25
11.2.1	Equipment siting and protection	26
11.2.2	Supporting utilities.....	26
11.2.3	Cabling security	26
11.2.4	Equipment maintenance.....	26
11.2.5	Removal of assets	26
11.2.6	Security of equipment and assets off-premises.....	26
11.2.7	Secure disposal or re-use of equipment	26
11.2.8	Unattended user equipment.....	26
11.2.9	Clear desk and clear screen policy.....	26
12	Operations security	27
12.1	Operational procedures and responsibilities	27
12.1.1	Documented operating procedures	27
12.1.2	Change management.....	27
12.1.3	Capacity management.....	28
12.1.4	Separation of development, testing and operational environments	29
12.2	Protection from malware.....	29
12.2.1	Controls against malware.....	30
12.3	Backup	30
12.3.1	Information backup.....	31
12.4	Logging and monitoring	31
12.4.1	Event logging	31
12.4.2	Protection of log information.....	32

12.4.3	Administrator and operator logs.....	32
12.4.4	Clock synchronisation.....	33
12.5	Control of operational software	33
12.5.1	Installation of software on operational systems	33
12.6	Technical vulnerability management	33
12.6.1	Management of technical vulnerabilities	33
12.6.2	Restrictions on software installation	34
12.7	Information systems audit considerations.....	34
12.7.1	Information systems audit controls	34
13	Communications security.....	35
13.1	Network security management.....	35
13.1.1	Network controls.....	35
13.1.2	Security of network services	35
13.1.3	Segregation in networks.....	36
13.2	Information transfer	36
13.2.1	Information transfer policies and procedures.....	36
13.2.2	Agreements on information transfer	36
13.2.3	Electronic messaging	36
13.2.4	Confidentiality or non-disclosure agreements	37
14	System acquisition, development and maintenance.....	38
14.1	Security requirements of information systems.....	38
14.1.1	Security requirements analysis and specification	38
14.1.2	Securing applications services on public networks.....	38
14.1.3	Protecting application services transactions.....	38
14.2	Security in development and support processes.....	38
14.2.1	Secure development policy	38
14.2.2	Change control procedures.....	39
14.2.3	Technical review of applications after operating platform changes	39
14.2.4	Restrictions on changes to software packages	39
14.2.5	System development procedures.....	39
14.2.6	Secure development environment.....	40
14.2.7	Outsourced development.....	40
14.2.8	System security testing.....	40
14.2.9	System acceptance testing.....	40
14.3	Test data	40
14.3.1	Protection of test data.....	40
15	Supplier relationships.....	41

15.1	Security in supplier relationship	41
15.1.1	Information security policy for supplier relationships.....	41
15.1.2	Addressing security within supplier agreements	41
15.1.3	Information and communication technology supply chain.....	41
15.2	Supplier service delivery management	42
15.2.1	Monitoring and review of supplier services.....	42
15.2.2	Managing changes to supplier services.....	43
16	Information security incident management	44
16.1	Management of information security incidents and improvements.....	44
16.1.1	Responsibilities and procedures.....	44
16.1.2	Reporting information security events.....	44
16.1.3	Reporting information security weaknesses	45
16.1.4	Assessment and decision of information security events	46
16.1.5	Response to information security incidents	46
16.1.6	Learning from information security incidents	46
16.1.7	Collection of evidence	47
17	Information security aspects of business continuity management.....	48
17.1	Information security continuity.....	48
17.1.1	Planning information security continuity.....	48
17.1.2	Implementing information security continuity	48
17.1.3	Verify, review and evaluate information security continuity	49
17.2	Redundancies	49
17.2.1	Availability of information processing facilities	49
18	Compliance	50
18.1	Information security reviews	50
18.1.1	Independent review of information security	50
18.1.2	Compliance with security policies and standards	50
18.1.3	Technical compliance inspection.....	50
18.2	Compliance with legal and contractual requirements	50
18.2.1	Identification of applicable legislation and contractual requirements	50
18.2.2	Intellectual property rights (IPR).....	51
18.2.3	Protection of documented information	51
18.2.4	Privacy and protection of personally identifiable information	51
18.2.5	Regulation of cryptographic controls.....	52
	Annex A: Cloud Computing Service Extended Control Set.....	53
	CLD.6 Organization of information security	53
	CLD.6.1 Internal organization	53

CLD.6.1.8 Management commitment to information security	53
CLD.6.1.9 Information security co-ordination	53
CLD.6.2 External parties.....	54
CLD.6.2.1 Identification of risks related to external parties.....	54
CLD.6.2.2 Addressing Security when dealing with customers	56
CLD.6.2.3 Addressing security in third party agreements.....	57
CLD.11 Communications and Operations	58
CLD.11.1 Operational procedures and responsibilities	58
CLD.11.1.5 System acceptance	58
CLD.11.2 Protection from malware.....	59
CLD.11.2.2 Controls against unauthorized mobile code	59
CLD.11.8 Logging and Monitoring	60
CLD.11.8.6 Audit logging	60
CLD.13 Access control	60
CLD.13.4 System and application access control.....	60
CLD.13.4.5 Sensitive System Isolation	60
CLD.13.5 Network access control	61
CLD.13.5.1 User authentication for cloud service connection	61
CLD.13.5.2 Equipment Identification in Cloud Networks	62
CLD.13.5.3 Network Connection Controls.....	62
CLD.13.5.4 Network routing control.....	63
CLD.13.6 Operating system access control	64
CLD.13.6.1 User identification and authentication	64
CLD.13.6.2 Session time-out	64
CLD.13.6.3 Limitation of connection time	65
CLD.14 System acquisition, development and maintenance.....	65
CLD.14.5 Correct processing in applications	65
CLD.14.5.1 Input data validation.....	65
CLD.14.5.2 Control of internal processing.....	66
CLD.14.5.3 Message integrity	67
CLD.14.5.4 Output data validation	67
CLD.17 Compliance	68
CLD.17.1 Compliance with legal and contractual requirements	68
CLD.17.1.7 Non-disclosure of communications.....	68
CLD.17.2 Compliance with information security policies and standards, and technical compliance	69
CLD.17.2.3 Monitoring System Use.....	69

CLD.17.3 Information systems audit considerations.....	70
CLD.17.3.2 Protection of information systems audit tools	70
CLD.17.3.3 Compliance Independent and Third party Audits	70
Annex B: Controls and Implementation Guidance for cloud consumer and cloud provider...	72
Annex C: Control Applicability by Service type	73
Annex D: Risk sources specific to cloud computing and cloud service	78
Bibliography	82

Foreword

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*.

0 Introduction

0.1 Overview

This International Standard provides guidelines supporting the implementation of Information security controls [JP1] for providers and users of cloud computing services. Selection of appropriate controls and the application of the implementation guidance provided will depend on a risk assessment as well as any legal, contractual, or regulatory requirements. ISO/IEC 27005 provides information security risk management guidance, including advice on risk assessment, risk treatment, risk acceptance, risk communication, risk monitoring and risk review. [AU3]

[WD1:DoC US4, US5, US6 Paragraph Deleted and aligned with Scope as per DoC]

0.2 Needs

One of the primary concerns with the use of cloud services is how cloud consumer can obtain services from cloud provider, in a manner which meets their security requirements. There is an industry wide knowledge gap concerning information choosing cloud services and how to evaluate their security posture.

[WD2:DoC CA8, US1]

0.3 Objectives

The objectives of this International Standard is to provide a security control framework and implementation guidance between cloud consumer and providers.

The guidelines of this International Standard include identification of risks and associated controls for the use of cloud service.

Adoption of cloud service is expected to reduce IT capital and operating cost. However, there are additional security considerations in order to leverage the anticipated benefits.

[WD2:DoC CA9]

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

[NWIP SC27 N10029]

[WD1:DoC SC27 N10593]

[WD2:DoC SC27 N11121]

[WD3:DoC SC27 N11915]

1 Scope

This International Standard gives guidelines for information security controls associated with cloud computing services by providing:

- a) additional implementation guidance for relevant information security controls specified in ISO/IEC 27002; and
- b) additional controls and implementation guidance that specifically relate to cloud computing services.

This International Standard provides implementation guidance for both providers and consumers of cloud computing services. *[AU4]*

[WD1:DoC US2, US3, US6 Proposed scope]

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, *Information technology - Security techniques - Code of practice for information security controls*

[WD2:DoC CA10, INLAC1]

[Editor's note: NB's response is requested on whether ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 17788, ISO/IEC 17789 are Normative reference or not. Decisions regarding normative references are postponed to the next meeting on April, 2013.[JP3]

3 Terms and definitions

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

[WD1:DoC US7, AU02, AU03, AU04. AU05 Terms and definitions]

[WD2:DoC CA7, CA12, CA13, US 13, US14, INLAC2, etc. based on Major issue(5)]

[WD2:DoC CA11]

[Editor's note: NB's and liaisons are requested on provide the terms which SC27/WG1 should define in addition to the terms defined by SC38..]

3.1 cloud computing

a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable resources (e.g. networks, servers and storage systems), applications and services that can be rapidly provisioned and released with minimal management effort or service provider interaction.

[ISO/IEC WD 17788]

3.2 cloud service

function useful to a **cloud consumer** (3.3) provided by a **cloud provider** (3.4)

[ISO/IEC WD 17788]

3.3 cloud consumer

person or organization that has a relationship with and uses services from **cloud providers** (3.4)

[ISO/IEC WD 17788]

[WD2:DoC JP4]

3.4 cloud provider

person, organization or entity responsible for making a service available to **cloud consumer** (3.3)

[ISO/IEC WD 17788]

[WD2:DoC JP3]

3.5 IaaS (Infrastructure as a Service)

capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications

NOTE The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

[ISO/IEC WD 17788]

3.6 PaaS (Platform as a Service)

capability provided to the consumer is to deploy onto the **cloud infrastructure** (3.X) consumer-created or acquired applications created using programming languages and tools supported by the provider

NOTE The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

[ISO/IEC WD 17788]

3.7 SaaS (Software as a Service)

capability provided to the consumer is to use the provider's applications running on a **cloud infrastructure** (3.X)

NOTE The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

[ISO/IEC WD 17788]

4 Overview

[WD1:DoC US6 the phrase “information security assurance framework” has been dropped].

4.1 Structure of this Guidance

[WD1:DoC US2, US8 Structure based on ISO/IEC27011]

[WD1:DoC AU01 Structure based on ISO/IEC27011]

This International Standard has been structured in a format similar to ISO/IEC 27002. In cases where objectives and controls specified in ISO/IEC 27002 are applicable without a need for any additional information, only a reference is provided to ISO/IEC 27002. Cloud service specific set of control and implementation guidance is described in Annex A (normative). *[WD2:DoC JP26]*

In cases where controls need additional guidance specific to cloud service, the ISO/IEC 27002 control and implementation guidance is not repeated, followed by the cloud service specific implementation guidance related to this control. *[WD2:DoC INLAC9]* Cloud service specific implementation guidance and other information are included in the following clauses:

- Security Policies (Clause 5)
- Organisation of information security (Clause 6)
- Human Resource Security (Clause 7)
- Asset management (Clause 8)
- Access Control (Clause 9)
- Cryptography (Clause 10)
- Physical and environmental security (Clause 11)
- Operations security (Clause 12)
- Communications security (Clause 13)
- Systems acquisition, development and maintenance (Clause 14)
- Supplier relationships (Clause 15)
- Information security incident management (Clause 16)
- Information security aspects of business continuity management (Clause 17)
- Compliance (Clause 18)

Each clause contains a number of main security categories.

Each main security category contains:

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

Control descriptions are structured as follows:

Control objective of ISO/IEC 27002

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

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

provides the description “Control 6.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

Sector-specific guidance for cloud computing services

provides following three types of description “The following sector-specific guidance also applies.”.

Type 1

Cloud Consumer	Cloud Provider

Type 2

Cloud Consumer

or

Cloud Provider

Type 3

Cloud Consumer	Cloud Provider

Other information for cloud computing

provides additional information that may need to be considered, when cloud consumer or cloud provider adopt cloud service.

4.2 Relations with the other standards

This International Standard contains overview, terms and definitions, control objectives, control, implementation guidance and other information descriptions. This can be applied with other ISMS family of standards for information security management systems as sector-specific standard .

[Editor's note: NB's and liaisons are requested on provide the texts which describes relationships between ISO/IEC 27017 and ISO/IEC 27036. [US3]

4.3 Models

4.3.1 General

The models of cloud computing consist of three service models and four deployment models.

4.3.2 Service model

Service models are categories of cloud services and are defined in ISO/IEC CD 17788 and ISO/IEC WD 17789 . There are primarily three such categories of cloud services: SaaS, PaaS, and IaaS. [US4]/[WD2:DoC CA21, US19, INLAC10, CA23, GB06, GB07]

4.3.3 Deployment model

Four deployment models of cloud computing are identified based on cloud infrastructure and services are defined in ISO/IEC WD 17788 and ISO/IEC WD 17789. They are Private cloud, Community cloud, Public cloud and Hybrid cloud.

4.3.4 Relations between cloud consumer and cloud provider

This International Standard is also applicable to cloud providers when they use other cloud service as means of their providing cloud service. In this case, the cloud provider is also a cloud consumer. The cloud consumer is primarily responsible for the security of information stored, transmitted and processed in the cloud services. The cloud consumer should be aware and the different deployment model and their characteristics in terms of information security.

[WD1:DoC CA5 Included guidelines]

4.4 Assessing security risks in cloud service

Security requirements are identified by a methodological assessment of security risks. Each cloud consumer [NZ4] is expected to complete its own information security risk assessment to determine impact to its business in relation to the likelihood of the information security exposure or controls failure. Expenditure on controls needs to be balanced against the business harm likely to result from security failures. The results of the risk assessment help to guide and determine the appropriate management action and priorities for managing information security risks, and for implementing controls selected to protect against these risks.

[WD1:DoC CA6]

Risk assessment should be run periodically but may as well be performed following the manifestation or observation of a vulnerability or new threat. The risk assessment may as well be conducted on a special ad hoc way or with special or specific conditions. *[ISACA2]*

- a) As a participant in the cloud eco-system, the risk posture of the organization has a direct impact on the commons of exchange of services and virtual assets. As such, it is a mandate that organizations communicate their risk measures to those who directly depend on their services and virtual assets;
- b) It is a recommendation that a commonly accepted measure for the communication of risk be adopted. An example of one such standard is the ISO 31000 Risk Management.

[WD2:DoC AU8, GB08, GB09]

Cloud consumer should consider the following when assessing *[US5, CSA5]* information security risks for use of cloud services. It should be noted that the factors listed below may affect types of risk that are beyond the scope of this standard as well as information security risk. *[WD2:DoC AU8]*

- a) Information security management of cloud consumer cannot reach *[US6]* the services directly, and risks can be increased or difficult to be measured.
- b) Use of cloud services causes change to the organization's information processing facilities and information services *[US7]*.
- c) Information regarding information security controls disclosed by cloud provider can be limited or abstracted *[US8]* in order to minimize risks to the cloud provider associated with the disclosure of details of controls. Cloud providers can offer to provide more detailed information to a current or prospective cloud consumer using a NDA or other legal document as protection of any disclosed information. *[CA3]*
- d) Disclosure of cloud provider security information, risks and vulnerabilities can expose all cloud consumers to risk due to the shared nature of the services. *[WD1:DoC CA2]*
- e) Failure to disclose a known vulnerability or exploit of the infrastructure poses a risk to the cloud consumer *[CA4]*
- f) The consumer should take into consideration of contractual risks that arise out of click wrap agreement in different jurisdictions. *[NZ5]*
- g) The consumer should take into account the legal risks that may not protect his rights in cloud provider jurisdiction *[NZ5]*
- h) The cloud consumer should take principles of good governance for protection of consumer rights in different jurisdiction by assessing the countries quality of rule of law. *[NZ5]*
- i) Risk can arise when cloud consumers and cloud providers are in different jurisdictions. For example:
 - risks (including but not limited to access to information by foreign governments) may arise when information is stored, transits, or is processed in a country or jurisdiction other than that of the cloud consumer;
 - risks may be associated with the use of encryption and what might happen to stored, encrypted information beyond the planned lifetime of the encryption technique used;
 - risks may be associated with loss of protection by local laws considering scenarios such as prosecuting a local company for practices at overseas data centres, and holding local company representatives accountable for the actions of separate overseas parts of their companies;
 - risk may be associated with local compliance requirements when the information is beyond the protection of local law and exposed to foreign sovereign risk; and
 - geo-political risks may be associated with differing and conflicting regulatory environments from data centre jurisdiction to jurisdiction.' *[WD1:DoC CA3]*

5 Security Policies

5.1 Management direction for information security

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

5.1.1 Policies for information security

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

Cloud Consumer
<p>The cloud consumer is responsible for developing its information security policy based on its security risk assessment. [WD1:DoC CA8]</p> <p><i>The cloud consumer is responsible for acquiring a detail and documented understanding of the cloud providers processing services including hypervisors, levels of virtualization, data flows, and their existing security administrative, technical, and other internal risks and controls over the cloud consumers information processing, privacy compliance, and data security.</i></p> <p><i>The cloud consumer is responsible for evaluating a cloud providers existing security capability and maturity level in detail data flow diagrams and processing points - as well as the cloud consumers data privacy compliance requirements and data breach notification needs and then matching the requirements and the capabilities before developing its information security policy based on its comprehensive cloud security risk assessment. [ISACA3]</i></p> <p>Information security policy should state information security implications in the use of cloud service, including:</p> <ul style="list-style-type: none"> a) scope of information security; b) risk management framework; c) definition of general and specific responsibilities for information security management; d) brief explanation of policy, principle and standards for business continuity management; e) brief explanation of policy, process and procedure related to incident management; [CA5.5]. f) brief explanation of policy, process and procedure related to vulnerability disclosure; [CA6] g) references to documentation which may support information security policy.

5.1.2 Review of the policies for information security

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

6 Organisation of information security

6.1 Internal organisation

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 Consumer	Cloud Provider
<p>Information security responsibilities of cloud consumer and cloud provider should be clearly documented and stated in information security policies, processes and service level agreements. [US11, ISACA5, US13]</p> <p>Cloud consumer should confirm the cloud provider's responsibilities on a periodic basis.</p> <p>Responsible management of business unit should be clearly identified, when the business unit is responsible for information security of cloud service in order to ensure appropriate safeguards are identified, implement controls or accept the associated risk. [ISACA6].</p>	<p>Information security responsibilities of the cloud provider should be clearly defined and documented with the cloud consumer. [US14]</p>

6.1.2 Contact with authorities

Control 6.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud Consumer	Cloud Provider
<p>Cloud consumer should identify the appropriate supervisory authorities, court of jurisdiction, relevant association and contact of cloud provider including backup and escalation points. [WD1:DoC CA14]</p> <p>Cloud consumer should add supervisory authority and relevant association to the contact list for information security incidents for cloud consumer in order to communicate with supervisory authority. [WD1:DoC CA13]</p> <p>Cloud consumer should identify and manage the support contact and the customer contact of the cloud provider.</p> <p>Cloud consumer should request information to</p>	<p>Cloud provider should maintain and provide the following contacts updated and make them available to the cloud consumer:</p> <ul style="list-style-type: none"> a) supervisory authority; b) court of jurisdiction of data centers, repositories and other relevant facilities under cloud provider's control; [WD1:DoC CA15] c) relevant association and contact of the cloud provider including backup, escalation points, support and customer contact. [JP6, NZ7, US16, ISACA14] <p>Cloud provider should identify and manage the customer contact of the cloud consumer contact of the cloud consumer. [ISACA13].</p>

the cloud provider to maintain the contacts updated. [JP5]	
--	--

6.1.3 *Contact with special interest groups*

Control 6.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

6.1.4 *Information security in project management*

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

6.1.5 *Segregation of duties*

Control 6.1.5 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud Consumer	Cloud Provider
Cloud consumer should request the cloud provider with information of privileges in the cloud service to segregate duties within the cloud consumer. [JP9, IE10]	<p>Cloud provider should provide the cloud consumer with the information of privileges in the cloud service to cloud provider to support segregation of duties within the cloud consumer. [JP10]</p> <p>The cloud provider must ensure it has adequate segregation of duties and responsibilities to the people who have access to information assets under the service we are paying the consumer cloud, so that anyone who is not who manages access. [ISACA31]</p> <p>Conflicting role combinations should be documented in a machine readable format and communicated to other participants in the supply chain. [WD1:DoC US21]</p> <p>Separation of development of the cloud provider [IE9] personnel should match the policy requirements of the cloud consumer [IE11] and the legal requirements of the cloud consumer's [IE11] physical jurisdiction. [WD1:DoC US22]</p>

6.2 *Mobile devices and teleworking*

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

6.2.1 Mobile device policy

Control 6.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud Consumer	Cloud Provider
Cloud consumer should treat security controls based on functionality of mobile devices, presuming use of mobile computing. Cloud consumer should request information to the cloud provider to manage to use cloud service from mobile computing. <i>[JP39]</i>	Cloud provider should provide the following information to the cloud consumer to manage to use cloud service from mobile computing: <ul style="list-style-type: none"> a) available type of mobile device; b) functional specifications of identifying and restricting connection of mobile device; c) functional specifications of the interface and application dedicated to mobile computing: <ul style="list-style-type: none"> 1) supported OS of mobile device; 2) provided services; d) specifications of encryption of communication between mobile device and cloud computing environment. <i>[JP40]</i>

6.2.2 Teleworking

Control 6.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud Consumer
Cloud consumer should establish and implement the policy, operational plans and procedures for teleworking activities with cloud service.

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 Consumer
<p>Cloud consumer should add following items to awareness, education and training programme for all employees, and contractors and third party users if applicable:</p> <ul style="list-style-type: none"> a) policy for use of cloud service; b) standards and procedures for use of cloud service; c) Information security risks and their treatment for each cloud service; d) risks of systems and network environment for use of cloud service. <p>Cloud consumer should consider cloud service in use and trainee's literacy level for awareness, education and training programmes.</p> <p>Cloud consumer should add awareness, education and training about its policy and procedure for use of cloud service as part of existing programme.</p>

7.2.3 *Disciplinary process*

Control 7.2.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud Provider
Disciplinary responsibilities of the cloud provider should match the policy requirements of the cloud consumer [IE11]. [WD1:DoC US17]

7.3 Termination and change of employment

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

7.3.1 *Termination or change of employment responsibilities*

Control 7.3.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud Provider
Termination responsibilities of the cloud provider personnel should match the policy requirements of the cloud consumer. [WD1:DoC US18].

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 Consumer	Cloud Provider
Cloud consumer should identify the names of cloud service and each of their providers, and document them in inventory of assets.	Cloud provider should provide the location of their assets along with their asset inventory. <i>[ISACA17]</i>

8.1.2 Ownership of assets

Control 8.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud Consumer	Cloud Provider
<p>The asset owner should be responsible for:</p> <ul style="list-style-type: none"> a) ensuring that information and assets associated with information processing are appropriately classified; b) defining and periodically reviewing policies, processes and procedures governing information processing as implemented by Cloud provider [IE9]s 	<p>Cloud provider [IE9]s should</p> <ul style="list-style-type: none"> a) Enforce access restrictions and classifications as dictated by the data owner, taking into account applicable access control policies. b) Provide automated transparency into information processing activities that directly or indirectly interact with data and assets belonging to an asset owner. c) Submit to audits as required by the asset/data owner <i>[WD2:DoC GB42]</i> d) Provide methods that indicate how data of cloud consumer who is no longer using the cloud provider is destroyed on all media and systems where their data was stored. <i>[CA7]</i> e) Submit to audits or provide acceptable audit reports from trusted third parties to meet the requirements of asset/data owners. <i>[ISACA 22]</i> <p>Ownership may be allocated to</p> <ul style="list-style-type: none"> a) a business process; b) a defined set of activities;

	c) an application; or d) a defined set of data
--	---

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. The following sector-specific guidance also applies.

Cloud Consumer
Cloud consumer should identify information to be located and acceptable use of the service based on the risk assessment of each cloud services. [ISACA23] All employees, contractors and third party users are contractually obligated to follow the rules that only authorized usage of the services is allowed. Disciplinary actions will occur if not followed. [ISACA24, US17]

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. The following sector-specific guidance also applies.

Cloud Consumer	Cloud Provider
Cloud consumer should add classifications considering cloud service to its classification guideline in consultation with cloud provider. Data, and objects containing data (e.g. laptops, iPhones, USB drives, physical media), should be assigned a classification based on data type, jurisdiction of origin, jurisdiction domiciled, context, legal constraints, contractual constraints, value, sensitivity, criticality to the organization and third party obligation for retention and prevention of unauthorized disclosure or misuse. [ISACA25]	Cloud provider should classify cloud consumer data at unless otherwise agreed [ISACA26]

8.2.2 *Labeling of information*

Control 8.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud Consumer	Cloud Provider
<p>Cloud consumer should establish and document procedures for labelling information which is shared with the cloud provider and is required for acquiring or using cloud services. [CSA6]</p> <p>Cloud consumer should request cloud provider to provide the information on functionality for labelling. [JP7]</p> <p>Cloud consumer should confirm procedures for identifying and separation of the consumers information.[SE05]</p>	<p>Cloud provider should provide the following information to the cloud consumer:</p> <ul style="list-style-type: none"> a) Functionalities for labelling, b) Functionalities to customize labelling. [JP8, ISACA29] <p>The cloud provider must provide procedures for labelling the information delivered, processed and stored in the cloud service that is being provided so as to ensure the guidelines or conditions provided by the cloud consumer.</p> <p>The cloud provider must have documented safe handling procedures for processing, storage, transmission occurring, sorting, delivery and destruction of information assets, and chain of custody and security incidents. [ISACA27]</p>

8.2.3 Handling of assets

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

8.2.4 Return of assets

Control 8.2.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud Consumer
<p>Cloud consumer should ensure that all employees, contractors and third party users return all of the organization's assets created or stored on cloud service at the termination of their employment, contract and agreement.</p> <p>Cloud consumers should ensure that arrangements are made for the return of proprietary data such as cloud consumer-owned databases contents, emails and intellectual property upon termination of employment, contract and agreement with the cloud provider. [ISACA35]</p> <p>The intent of the guidance may be achieved by simply revoking access to the virtual assets. (See 8.3.3) [WD2:DoC CA92].</p>

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. The following sector-specific guidance also applies.

Cloud Consumer	Cloud Provider
<p>Cloud consumer should develop an access control policy in the light of access control functionality provided by the cloud service taking into consideration: [WD2:DoC CA104, US63]</p> <ul style="list-style-type: none"> a) segregation of access control roles b) authorization process for access request, e.g. management procedures of user profiles; c) access control rights applied in cloud service. <p>Cloud consumer should request information about access control functionality to the cloud providers to develop an access control policy in cloud service. [JP41]</p>	<p>Cloud provider should provide the following information about access control functionality to the cloud consumer to develop an access control policy in cloud service:</p> <ul style="list-style-type: none"> a) segregation of access control roles; b) authorization process for access request, e.g. management procedure of user profiles <p>[JP42]</p> <p>Security assessment should be performed by cloud provider in the cloud environment to identify the opportunity for back door access to cloud consumer's information assets and software. [ISACA76]</p>

9.1.2 Policy on the use of 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 Consumer	Cloud Provider
<p>Cloud consumer should include the following [US64] regarding the use of cloud service in the policy on the use of network services: [WD2:DoC CA115]</p> <ul style="list-style-type: none"> a) access control for each cloud consumer to the services provided by cloud provider; b) access controls preventing network access from designated sites or environments to the cloud service.. c) End-point network connectivity health-checks [CSA23] 	<p>Cloud provider should provide the specification on type of information for the purpose of restricting network access control to the cloud consumer including:</p> <ul style="list-style-type: none"> a) user id and application service used by cloud consumer; b) domain name, IP address and port number of cloud provider. <p>[JP44]</p>

Cloud consumer should request the specification on type of information for the purpose of restricting network access control to the cloud provider. [JP43]	
--	--

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. The following sector-specific guidance also applies.

Cloud Consumer	Cloud Provider
<p>Cloud consumer should include a [US67] formal procedure of registration and de-registration of user IDs of cloud services in place for granting and revoking access to all information systems and services.</p> <p>[WD2:DoC CA120]</p> <p>Cloud consumer should confirm that formal user registration and de-registration procedures (e.g. registration and de-registration of user IDs of cloud services) are performed by the functionality provided by the cloud provider. [WD2:DoC CA119]</p> <p>[Order changed US66]</p> <p>Cloud consumer should request information to the cloud provider to ensure user registration on the cloud service.[JP45]</p>	<p>Cloud provider should provide the following information to the cloud consumer to ensure user registration and de-registration on the cloud service:</p> <ul style="list-style-type: none"> a) user registration procedures; b) information required for user registration; c) specification of user identification code; d) functionality for user identification; e) specifications of user management tools when those are provided as part of the cloud service. f) mechanisms and procedures used to verify user identity using unique identifier provided [CSA24], [JP46]

9.2.2 Privilege management

Control 9.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud Consumer	Cloud Provider
----------------	----------------

<p>Cloud consumer should confirm that procedures of restricting and controlling the allocation and use of privileges are realized on cloud service. [WD2:DoC CA125]</p> <p>Cloud consumer should request information to the cloud provider to ensure privilege control on cloud service. [JP47]</p>	<p>Cloud provider should provide the following information to the cloud consumer to ensure privilege control in the use of cloud service:</p> <ul style="list-style-type: none"> a) types and roles of privileges; b) functional specification of monitoring and controlling the use of privileged accounts; c) log of privileged accounts use. [JP48, US69]
---	---

9.2.3 Management of secret authentication information of users

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 Consumer	Cloud Provider
<p>Cloud consumer should confirm that formal management process for allocating of password is realized by the functionality provided by the cloud provider.</p> <p>Where password management tools and processes are part of the cloud service, the cloud consumer should confirm that formal management process for allocating of password is realized by the functionality provided by the cloud provider. [WD1:DoC CA42]</p> <p>Cloud consumer should request information to the cloud provider to ensure password management on cloud service. [JP49]</p>	<p>Cloud provider should provide the following information to the cloud consumer to ensure password management on cloud service:</p> <ul style="list-style-type: none"> a) procedures of issuance, change and re-issuance password; b) functional specification of password quality controlled by cloud consumer; c) functional specification for mistyping password procedure (e.g. lock function); d) Development of strong cloud-based authentication and authorization architecture and mechanisms <p>(including strong two-factor authentication techniques)</p> <ul style="list-style-type: none"> e) Detection method to proactively monitor unauthorized activities f) Strong cloud-based authentication and authorization architecture and mechanisms used by the cloud provider (including multi-factor authentication techniques); [CSA26] g) Guideline how to securely use account credentials between users and providers h) Confirmation that secret information will

	<p>never be stored. Description of secret validation process without storing the secret and protection measures against unauthorized access to i.e. “password hashes” or “password encryption”; [CSA26, ISACA78]</p> <p>Where password management tools and processes are part of the cloud service, the cloud consumer should confirm that formal management process for allocating of password is realized by the functionality provided by the cloud provider. [JP50]</p>
--	--

9.2.4 Review of user access rights

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

Cloud Consumer	Cloud Provider
Cloud consumer should request information on functional specification of listing the access rights by each user of cloud service to the cloud provider to review access rights. [JP51]	Cloud provider should provide information on functional specification of listing the access rights by each user of cloud service to support the cloud consumer in reviewing access rights. [JP52]

9.2.5 Removal or adjustment of access rights

Control 9.2.5 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud Consumer	Cloud Provider
<p>Cloud consumer should add procedures for access right management for each cloud service, including the documenting of the provider functionalities or services for access rights transfer and removal at the termination of employment, contract and agreement, or updating upon change. [US21]</p> <p>Cloud consumer should request cloud provider information about functionalities or services for removal or adjustment of consumer's access rights. [JP11]</p>	<p>Cloud provider should provide functionalities or services for removal or adjustment of consumer's access rights. [JP12]</p> <p>The cloud provider must ensure that procedures for administering access rights that are given to them, will be executed according to the letter the guidelines defined, if required change, addition or modification of any right of access that endangers administration of assets under custody shall have a documented procedure that event information to the cloud consumer who must implement the changes is properly accompanied and followed all protocol changes. [ISACA37]</p> <p>Cloud provider should provide information about functionalities or services for cloud consumer to transfer access right. [ISACA38]</p>

9.3 User responsibilities

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

9.3.1 Use of secret authentication information

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

9.4 System and application access control

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

9.4.1 Information access restriction

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

Cloud Consumer	Cloud Provider
Cloud consumer should restrict access to cloud service by cloud consumers and support personnel in accordance with the organizational access control policy (see 13.1.1) Cloud consumer should request to the cloud provider with specifications of access restrictions to the cloud consumer's information. [JP53]	Cloud provider should provide the following information to the cloud consumer for access restriction on its assets: a) relevant services that have access to the cloud consumer's information maintained in the cloud service: 1) service type; 2) functional specification of controls to restrict access to the information; b) specifications of controls to restrict access by cloud provider to the information. [JP54]

9.4.2 Secure log-on procedures

Control 9.4.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud Consumer	Cloud Provider
Cloud consumer should confirm that a log-on procedure provided on cloud service is [US72]secure. Cloud consumer should request the detail specifications of log-on procedure to the cloud provider to confirm that the procedure provided on the cloud service is [US72] secure. [JP55]	Cloud provider should provide the detail specifications of log-on procedure to the cloud consumer to support the cloud consumer in confirming that the procedure is [US72] secure. [JP56]

9.4.3 Password management system

Control 9.4.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud Consumer	Cloud Provider
<p>Cloud consumer should confirm that systems for managing password of cloud service are interactive and ensure quality passwords.</p> <p>Cloud consumer should request the information about specifications of password management system of the cloud service to the cloud provider to confirm that the system satisfies security functions required. [JP57]</p>	<p>Cloud provider should provide the specifications of password management system of the cloud service o confirm that the system satisfies security functions that cloud consumer required. [JP58]</p>

9.4.4 Use of privileged utility programs

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

Cloud Consumer
<p>Cloud consumer should restrict and should tightly control the use of utility programs that might be capable of overriding system and application controls</p> <p>Cloud consumer should request the following information to the cloud provider to restrict and control the use of utility programs accessing cloud service:</p> <ul style="list-style-type: none"> a) specifications of utility programs that might be capable of overriding system and application controls; b) functional specifications to restrict and control utility programs. [US75]

9.4.5 Access control to program source code

Control 9.4.5 and the associated implementation guidance and other information specified in ISO/IEC 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 Consumer	Cloud Provider
<p>Cloud consumer should confirm that functionalities of cryptography provided on cloud service are adequate with the policy on the use of cryptographic controls on cloud service.</p> <p>Cloud consumer should request information to the cloud provider to confirm that encryption functionalities provided on cloud service are adequate with the cryptographic policy on the use of cryptographic controls. [JP35, US59]</p>	<p>Cloud provider should provide the following information for cloud consumer to confirm that encryption functionalities provided on cloud service are adequate with the cryptographic policy:</p> <p>a) functional specifications of encryption used in cloud service provided by cloud computing provider, including:</p> <ul style="list-style-type: none"> 1) type, strength and quality of encryption algorithm; 2) object of encryption; <p>b) functional specifications of encryption on cloud service for cloud consumer, including:</p> <ul style="list-style-type: none"> 1) type of encryption algorithm, and strength and quality; 2) usage of encryption. [JP36, ISACA74]

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 Consumer	Cloud Provider
<p>Cloud consumer should identify cryptographic keys managed on cloud service, and establish the procedure of key management. Cloud consumer should request the following information on procedures used to manage keys related to cloud service:</p> <ul style="list-style-type: none"> a) specification of keys; b) specifications of key management system, including procedures for each process of key life-cycle i.e. generating, changing or updating, exchanging, storing, reading, revoking, recovering, archiving and 	<p>Cloud provider should provide the following information on key management service to support the cloud consumer in use of the service.:</p> <ul style="list-style-type: none"> a) type of keys; b) specifications of key management system, including procedures for each process of key life-cycle i.e. generating, changing or updating, exchanging, storing, revoking,

destroying; c) recommended key management procedures for use by customer.” [CSA20, JP37]	recovering, archiving and destroying; c) recommended key management. [JP38]
---	--

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. The following sector-specific guidance also applies.

Cloud Provider
Physical security responsibilities of the cloud provider [IE9] personnel should match the policy requirements of the cloud consumer [US22] and legal requirements of the cloud consumer's [US22] physical jurisdiction. [WD1:DoC US19]
Requirements on physical security perimeters should conform to the policy requirements of the cloud consumer. [JP13]

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 office, room 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.

11.2.4 Equipment maintenance

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

11.2.5 Removal of assets

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

11.2.6 Security of equipment and assets off-premises

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

11.2.7 Secure disposal or re-use of equipment

Control 11.2.7 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

11.2.8 Unattended user equipment

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

11.2.9 Clear desk and clear screen policy

Control 11.2.9 and the associated implementation guidance and other information specified in ISO/IEC 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. The following sector-specific guidance also applies.

Cloud Consumer	Cloud Provider
<p>Cloud consumer should develop and document operation procedures for the cloud consumer's use of a cloud service incorporating the cloud provider's support contact, topology reference designs and user manuals. [US32, ISACA51]</p> <p>Cloud consumer should request the following information from the cloud provider to develop operating procedures of the cloud service: [JP16, ISACA53, ISACA54]]</p> <ul style="list-style-type: none"> a) user manuals of cloud service; b) support contact; c) cloud provider topology reference designs showing generalized DC and network locations/connections/jurisdictions and redundancy provisions; [JP16] d) shared client services e.g. SAN backups, firewall and IDS management. [ISACA52] <p>[WD1:DoC CA26]</p>	<p>Cloud provider should provide the following information to support cloud consumer in developing operating procedures for the use of cloud services:</p> <ul style="list-style-type: none"> a) user manuals of cloud services; b) support contact c) cloud service topology designs showing generalized data center and network locations and connections. [JP17, US35, ISACA50]

[Editor's note: US NB is requested to provide contributions for US33, US34 and US36 comment in Rome editing meeting.]

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 Consumer	Cloud Provider
----------------	----------------

<p>Cloud consumer should manage changes by cloud provider on systems and services that affect information security of cloud consumer's organization within cloud consumer's change management process. Security attestations related to systems and services which represent shared infrastructure with other cloud consumers should be received from the cloud provider. [US38, WD1:DoC CA27]</p>	<p>Cloud provider should provide the following information regarding changes to the systems and services that affect information security of cloud consumer's organization for cloud consumer to manage changes: [ISACA57]</p> <ul style="list-style-type: none"> a) planned date and time of system changes; b) details of system changes: <ul style="list-style-type: none"> 1) application of new software or software patches; [ISACA59] 2) hardware changes; 3) network changes; 4) software changes; 5) changes to services; 6) changes to sub-provider; 7) physical relocation of systems; 8) risk assessment on the changes; [ISACA55] c) announcement of system change start and completion; d) acknowledgement or approval according to existing agreement; [ISACA58]
--	--

Other information for cloud computing

In case cloud consumer provides services to the internal or external users using cloud service, the cloud consumer may request the information of changes in the systems and services to the cloud provider to maintain provision of service specifications and levels. Example of this case is a SaaS provider relying upon IaaS.

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 Consumer	Cloud Provider
<p>Cloud consumer should confirm that the capacity that it has agreed to obtain from the cloud service is sufficient to deliver the cloud consumer's required system performance.</p> <p>Cloud consumer should monitor its own usage of cloud service resources and reconfigure its usage of those resources so that the cloud consumer's requirements for access-network and system performance can be met.</p> <p>Cloud consumer should project its future system performance requirements and use</p>	<p>Cloud provider should provide the following information to the cloud consumer to enable its capacity management:</p> <ul style="list-style-type: none"> a) system environment: <ul style="list-style-type: none"> 1) capacity of data storage; [WD2:DoC GB96] 2) capacity of network and network equipment including the virtual network in the cloud service environment (e.g., bandwidth, maximum number of network sessions); 3) lead time to have additional capacity or

<p>those to ensure availability of sufficient cloud service capacity. This may involve selection of an additional or replacement cloud service provider if the projected requirements exceed the capacity available from a current cloud provider. [US39]</p> <p>Cloud consumer should confirm that a cloud provider can deliver the capacity and required and future system performance for a cloud service. The following should be considered when determining if a cloud provider can manage the capacity and system performance:</p> <p>a) system environment;</p> <ol style="list-style-type: none"> 1) data storage 2) capacity of network and network equipment including the virtual network in the cloud service environment (e.g, bandwidth, maximum number of network sessions); 3) agreed or expected system performance 4) lead time to have additional capacity or system performance, and minimum unit of the addition 5) maximum capacity and system performance; 6) redundancy and diversity of systems 7) redundancy and diversity of access networks <p>b) statistics on system resource usage</p> <ol style="list-style-type: none"> 1) statistics in a given time period 2) maximum system resource usage <p>[US40]</p>	<p>system performance, and minimum unit of the addition;</p> <p>4) maximum capacity and system performance;</p> <p>b) statistics on system resource usage:</p> <ol style="list-style-type: none"> 1) statistics in a given time period; 2) maximum system resource usage.[JP19] <p>c) lead time to provision additional resources (storage, CPU, database virtual machines, etc...) to cloud consumer, and minimum unit of addition;</p> <p>d) Limitations on additional resource provisioning to cloud consumer;</p> <p>e) Statistical information on resource provisioning failures either relating to specific cloud consumer account or service-wide, as well as average resource provisioning times. [CSA10]</p>
--	---

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. The following sector-specific guidance also applies.

Cloud Consumer
Cloud consumer should use virtual environments to separate development, test and operational environments where applicable. [JP20]

12.2 Protection from malware

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

12.2.1 Controls against malware

Control 12.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud Consumer	Cloud Provider
<p>Cloud consumer should confirm measures of cloud provider against malware, and implement its own measures if needed. Cloud consumer should confirm reporting procedure for malware infection at any cloud consumer [JP21]</p> <p>Cloud consumer should request the following information to the cloud provider.</p> <ul style="list-style-type: none"> a) Security-related configuration and options to be used. b) System components covered by security controls and configuration elements (e.g. does it include network components, guest OS layers etc.). c) Selection, schedule and information on software updates and patches to be applied, e.g. what patches, patching frequency and covered systems. d) Criteria and procedures for vulnerability discovery, reporting and remediation. Specific vendor-approved lists, public databases or approved penetration testing tools used. e) Incident response and recovery procedures in case of an infection of different cloud components like the neighbor VM, the VMM or the cloud management plain [CSA12] f) consumer to implement own measures against malicious codes: [ISACA60] <p>Additionally, service level reports should be provided including:</p> <ul style="list-style-type: none"> a) Information on patches and controls in place versus open vulnerabilities b) Information on compensating controls applied c) Data on specific vulnerabilities and trends, such as their classification and severity scores, including for the virtualization layer and its managements systems 	<p>Cloud provider should provide the following information to the cloud consumer to help evaluating measures applied at the provider and implementing its own measures against malware:</p> <ul style="list-style-type: none"> a) measures against malware including frequency of updating of malware detection and repair software and its signatures; and b) subscription to intelligence and reputation-services about suspicious IP addresses and networks; [JP22] c) the reporting procedure for malicious code infection; [US41] d) disclose vulnerabilities that have been discovered in the cloud provider's infrastructure. This might be related to either proprietary software or that provided by a 3rd party provider. [CA9] <p>If the measures used by the provider are not adequate based on the information security policy, then additional measures should be implemented. [US41]</p>

12.3 Backup

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

12.3.1 Information backup

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

Cloud Consumer	Cloud Provider
<p>Cloud consumer should define back-up policy, and develop procedures considering the followings:</p> <ul style="list-style-type: none"> a) back-up and restoration functions of the cloud service; b) back-up and restoration functions that need be developed by the cloud consumer. c) at least 128-bit encryption should be used on back-ups d) local and or off-site storage of back-ups should be documented [ISACA63] e) retention period for back-up data [ISACA62] 	<p>Cloud provider should provide the following specifications of back-up function to the cloud consumers to support developing cloud consumer's back-up policy and procedures:</p> <ul style="list-style-type: none"> a) scope of back-ups; b) back-up methods and data formats; c) version control for back-up data; d) governing jurisdictions; e) procedure to verify integrity of back-up data; f) procedure to restore from back-up; [JP23, ISACA61] g) procedure to test functionality of complete back-up routines; [SE06] h) Provide a real-time portal or console view of the backup systems [US46]

12.4 Logging and monitoring

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

[Editor's note: US NB is requested to provide contributions for US54 and US55 comment in Rome editing meeting.]

12.4.1 Event logging

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

Cloud Consumer	Cloud Provider
<p>Cloud consumer should request the following from the cloud provider:</p> <ul style="list-style-type: none"> a) Available logging information [CSA17] <p>Cloud consumer should define the requirements on fault logging on the cloud service, and confirm that the requirements are implemented and the logs are provided to the cloud consumer. Cloud consumer should analyze fault logs and take appropriate actions.</p>	<p>Cloud provider should include the scope of events from the virtualization layer into their SIEM system. [CSA18]</p> <p>Cloud provider should provide the following specifications to the cloud consumer to support checking if the requirements are implemented:</p> <ul style="list-style-type: none"> a) events to be logged; b) information and data format to be

<p>Cloud consumer should request the specifications about event logging to the cloud providers to confirm if the requirements are implemented. [JP31]</p> <p>For each cloud service, the requirements for fault logging should be defined. Confirmation with the cloud provider that the requirements are implemented and logs to be provided to the cloud consumer. Fault logs for each cloud service should be analysed and appropriate actions taken. [US58]</p>	<p>recorded as fault logs;</p> <p>c) retention period of fault logs;</p> <p>d) interactively accessible period;</p> <p>e) method of verifying integrity of fault logs. [JP32]</p>
---	---

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. The following sector-specific guidance also applies.

Cloud Consumer	Cloud Provider
<p>Cloud consumer should confirm the service specifications that the logs and logging function are protected against unauthorized modification and access and that the retention periods are clearly defined. [ISACA70]</p> <p>Cloud consumer should request information on protection of logs to the cloud providers to confirm the logs are appropriately protected. [JP27]</p>	<p>Cloud provider should provide the following information to the cloud consumer to assure the logs are appropriately protected: [JP28, ISACA69]</p> <p>a) protection policy of logs;</p> <p>b) overview of log protection function.</p>

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. The following sector-specific guidance also applies.

Cloud Consumer	Cloud Provider
<p>Cloud consumer should confirm specification and availability of non-repudiation mechanisms such as signed third party time-stamps and Write-Once-Read-Many devices. [CSA19]</p> <p>Cloud consumer should request the presentation of the specification of operator logs to the cloud provider in the case they are not made available. [JP29]</p>	<p>Cloud provider should provide the specification of operator logs to the cloud consumer in case they are not made available. [JP30]</p>

12.4.4 Clock synchronisation

Control 12.4.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud Consumer	Cloud Provider
Cloud consumer should synchronize clocks in all information systems of the organization with clock in cloud service. Where the synchronization is impracticable, time differences should be recorded.	Cloud provider should provide information on the methods of presenting clocks of the cloud services to the cloud consumer. [JP34] [ISACA73]

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 Consumer	Cloud Provider
Cloud consumer should understand technical vulnerability management of cloud service. In case that the management is not compliant with cloud consumer' requirements, cloud consumers' own response should be considered. Cloud consumer should request the following information to the cloud provider to understand technical vulnerability management. a) way to identify technical vulnerability; b) policy to respond technical vulnerability; c) acceptance level of vulnerability assessment by cloud consumers; [JP64] d) request and agree upon criteria for system feature to be considered vulnerable	Cloud provider should provide the following information on technical vulnerability management: a) way to identify technical vulnerability; b) policy to respond technical vulnerability; c) acceptance level of vulnerability assessment by users. [JP65]

<p>Policies and procedures should be established and mechanism implemented for vulnerability and patch management, ensuring that application, system, and network device vulnerabilities are evaluated and vendor-supplied security patches applied in a timely manner taking a risk-based approach for prioritizing critical patches. [WD1:DoC US78][JP64]Cloud provider should not provide the cloud consumer of other cloud consumers vulnerabilities. [WD1:DoC CA48]</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.

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. The following sector-specific guidance also applies.

Cloud Consumer

<p>Cloud consumer should define the audit policy for cloud service. Cloud consumer should conduct an audit of the cloud service.</p>
--

Other information for cloud computing

Cloud consumer can confirm audit report by cloud provider, instead of conducting audit by oneself.

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. The following sector-specific guidance also applies.

Cloud Consumer	Cloud Provider
Cloud consumer should establish the mechanism to manage usage of cloud service through networks that are not managed by cloud consumer. [US44]	Cloud provider should provide the following information to the cloud consumer to support managing use of networks:
Cloud consumer should establish remote access to cloud services through private network or encrypted communication channel, where feasible. [WD1:DoC CA35, ISACA65]	a) Autonomous System Number (ASN) or ISP-assigned IP range;
Cloud consumer should request information on network service to the cloud providers to manage usage of networks that are not managed by cloud service use. [JP24]	b) network service provider in use;
	c) network subscription(s) information such as bandwidth service levels and diversity; [JP25]d) (D)DoS protection mechanism in place [CSA13, ISACA67]

Other information for cloud computing

Usage of cloud service may be permitted through networks that are not managed by cloud consumer, e.g., public network, even if the service is for internal use. In these cases, risk assessments should be performed prior to adoption. The cloud consumer should agree to number of audit's/assessments that can be conducted over the period of the contract. [WD1:DoC CA37]

Cloud provider should offer a real-time portal or console view to the availability of the cloud infrastructure. [WD1:DoC CA38]

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. The following sector-specific guidance also applies.

Cloud Consumer	Cloud Provider

[Editor's note: US NB is requested to provide contributions for US47 comment in Rome editing meeting.]

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 Consumer	Cloud Provider
<p>Cloud consumer should consider the need to request segregation in networks of the cloud provider. [US48]</p> <p>Cloud consumer should consider end-to-end encryption of traffic at the application layer, where proper network- or interface segregation can't be achieved. [CSA15]</p> <p>Cloud consumer should request information on functional specifications on dividing the networks into separate network domains, to the cloud provider to segregate networks of cloud service. [JP26]</p>	<p>The cloud provider should enforce logical segregation of networking between cloud consumers, for both access and for networking between virtualized resources within the cloud (e.g. VMs on VLANs). There should also be segregation between the networks used to access the cloud services, and the network used to administer and manage the cloud internally to the provider. [IE21]</p>

[Editor's note: US NB is requested to provide contributions for US48 and US50 comment in Rome editing meeting.]

Other information for cloud computing

Examples of cases when requesting cloud provider to segregate in networks are:

- a) competitors within the same industry co-exist within same cloud environment;
- b) when regulatory requirements dictate segregation/isolation of network traffic [US51]

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.

13.2.3 Electronic messaging

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

13.2.4 Confidentiality or non-disclosure agreements

Control 3.2.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud Consumer	Cloud Provider
<p>Cloud consumer should request cloud provider to provide a draft agreement prior to concluding confidentiality or non-disclosure agreements.</p> <p>Cloud consumer should ensure that agreement with the cloud provider includes clauses which satisfy requirements for confidentiality or non-disclosure agreements. Cloud consumer should have confidentiality or non-disclosure agreements separately when required. Cloud consumer should ensure agreement with the cloud provider include a definition of the information to be protected including classification and associated regulatory requirements. <i>[WD1:DoC CA12]</i></p> <p>Relevant operational procedures should be referenced in any confidentiality agreement. <i>[WD1:DoC US12]</i></p> <p>Information must not be loaded to the cloud before the confidentiality or non-disclosure agreements are signed. <i>[ISACA10]</i></p> <p>Cloud Consumer's Legal Counsel should review and provide feedback on the agreement. <i>[ISACA12]</i></p>	<p>Cloud provider should provide draft agreement to cloud consumer prior to concluding confidentiality or non-disclosure agreements. <i>[NZ6, US15]</i></p> <p>The cloud provider must keep updated records of monitoring conducted as to create security incidents, which must be submitted to the competent authorities at the time that they are required. If a cloud provider is attacked,, the providers should notify third parties, such as Internet or telecommunications operators to take action against the source of attack or be prepared for such events and inform relevant entities fraud or attempts information assets against the cloud consumer. <i>[ISACA 11]</i></p> <p>Cloud provider should ensure that confidentiality or non-disclosure agreements are signed by its employees and subcontractors. <i>[ISACA 9]</i></p>

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 Consumer	Cloud Provider
<p>Cloud consumer should specify the security requirements for the cloud service.</p> <p>Cloud consumer should analyze and evaluate the alignment of the implemented controls in cloud service to the requirement.</p> <p>Cloud consumer should reconsider use of the cloud service or other controls to be implemented, considering the identified risks by the analysis and evaluation.</p> <p>Cloud consumer should request the information related to the implemented control of cloud service to the cloud provider to analyze the alignment of control treatment between cloud consumer's requirement and the implemented controls in cloud service. [JP59]</p>	<p>Cloud provider should provide information related to the implemented controls of cloud service to the cloud consumer to support analysing the alignment of control treatment between cloud consumer's requirement and the implemented controls in cloud service. [JP60]</p>

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 *Change control procedures*

Control 14.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud Consumer

Cloud consumer should include change control for cloud service into change control procedures. [Cloud consumer should request the following information on change management to cloud provider to include change control for cloud service into change control procedures:

- a) contents of notification for change;
- b) methods of notification for change;
- c) timing of notification for change;
- d) risk assessment of change; [ISACA79]
- e) documented authorization, testing and approvals prior to implementation;
- f) back out procedures [JP59, ISACA80]

Cloud consumer should request protection measures against service disruption caused by user installed software (compute resource overload, network overload, misuse of IP address space (i.e. by spam). [CSA31]

14.2.3 *Technical review of applications after operating platform changes*

Control 14.2.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud Consumer

Cloud consumer should carry out technical review of applications managed by cloud consumer after operating system is changed on cloud service.
Cloud consumer should request the change information of operating system of cloud service to cloud provider to carry out technical review of applications managed by cloud consumer. [JP61]

14.2.4 *Restrictions on changes to software packages*

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

14.2.5 *System development procedures*

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

14.2.6 Secure development environment

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

14.2.7 Outsourced development

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

14.2.8 System security testing

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

14.2.9 System acceptance testing

Control 14.2.9 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud Consumer	Cloud Provider
<p>Cloud consumer should establish acceptance criteria of cloud service (see 6.1.2).</p> <p>Cloud consumer should carry out adequate system testing prior to acceptance of cloud service.</p> <p>Cloud consumer should request information to the cloud providers to select a cloud service. <i>[JP62, US77]</i></p>	<p>Cloud provider should provide the following information to the cloud consumer to select a cloud service:</p> <p>a) service level agreement;</p> <p>b) Business Associate Agreement;</p> <p>c) trial use specifications, including fees, trial period and disclaimer. <i>[JP63]</i></p>

[Editor's note: The definition regarding "Business Associate Agreement" is needed.]

14.3 Test data

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

14.3.1 Protection of test data

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

15 Supplier relationships

[Editor's note: US NB is requested to provide contributions for US23 comment in Rome editing meeting.]

15.1 Security in supplier relationship

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

15.1.1 Information security policy for supplier relationships

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

Cloud Consumer	Cloud Provider

[Editor's note: US NB is requested to provide contributions for US24 and US25 comment in Rome editing meeting.]

15.1.2 Addressing security within supplier agreements

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

Cloud Provider
Service Delivery of the cloud provider should match the policy requirements of the cloud consumer and the legal requirements of the contract between the provider and the consumer of the cloud consumer's physical jurisdiction. <i>[WD1:DoC US23, US24], [WD2:DoC GB85, GB86, GB87]</i>
Multi party agreements should reflect the responsibilities of the cloud provider and should be binding on all parties upon which the service offers depend. <i>[WD1:DoC US38]</i>

[Editor's note: US NB is requested to provide contributions for US26, US27 and US28 comment in Rome editing meeting.]

15.1.3 Information and communication technology supply chain

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

Cloud Provider
Security policy changes with material operational impact should require formal notification of subcontractors, tenants, supporting service tiers and employees of the impact and ramifications. Executive and line management should take formal action to support information security through clear documented direction, commitment, explicit assignment and verification of assignment

execution. [WD1:DoC US10]

[Editor's note: US NB is requested to provide contributions for US29 comment in Rome editing meeting.]

15.2 Supplier service delivery management

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

15.2.1 Monitoring and review of supplier services

Control 10.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud Consumer	Cloud Provider
<p>Cloud consumer should regularly monitor and review the services, reports and records provided by the cloud provider.</p> <p>Cloud consumer should regularly audit cloud provider's performance in accordance with the service agreement.</p> <p>Cloud consumers should be aware of the security requirements and confidentiality agreements of the cloud providers before conducting an audit. [ISACA40]</p>	<p>The cloud provider should provide the following information for the cloud consumer to monitor and review on a regular basis: [US30, JP14]</p> <ul style="list-style-type: none"> a) specific report on services operation regarding information security ; b) information security audit report c) service level report; d) trouble occurrences of the services; e) information security incidents affecting cloud consumer's distinct users f) information security certifications g) changes to the information security functions of the services h) implementation and operation reports of customized security controls". i) information security incidents and root cause problems affecting cloud consumer's distinct users; [ISACA42] j) Resolution / Corrective action of any identified action items needs to be documented. [ISACA 43]

15.2.2 Managing changes to supplier services

Control 10.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud Consumer	Cloud Provider
<p>Cloud consumer should follow and take required actions on changes by cloud provider on systems and services that affect information security of cloud consumer's organization within cloud consumer's change management process. [WD2:DoC CA96]</p>	<p>As a part of the cloud provider's change management process, the cloud provider should provide the following information to the cloud consumer regarding any changes to the cloud provider's systems and services that may affect the cloud consumer's information security:</p> <ul style="list-style-type: none"> a) planned date and time of system changes; b) details of system changes: <ul style="list-style-type: none"> 1) application of software patches; 2) hardware changes; 3) network changes; 4) software changes; 5) changes to services; 6) changes to sub-providers; 7) physical relocation of systems; c) announcement of system change start and completion. d) acknowledgement or approval according to existing agreement. [ISACA 47] <p>These changes should include the ones caused by the changes to the systems and services of other providers in the chain that affect consumer's information security through the services of the provider in direct relationship with the consumer. [US31.JP15] Changes to cloud provider systems should include an impact statement of the proposed change will impact the cloud consumers information assets stored in the systems experiencing the change. In addition if any data must be converted to a new platform, a documented reconciliation of the data must be performed by the cloud consumer to ensure no unintentional data loss or change has occurred during conversion. [ISACA48]</p> <p>Supply chain impacts on dependant services (See ISO27036-5)</p>

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 Consumer	Cloud Provider
Cloud consumer should develop criteria and procedure to inform providers about information security incident. Cloud consumer should request information to the cloud provider to develop criteria and procedure to inform providers about information security incident and to have report of information security incident. <i>[JP66]</i>	Cloud provider should provide the following information to the cloud consumer support developing criteria and procedure to inform providers about information security incident: <ul style="list-style-type: none"> a) contacts; b) contact method. Cloud provider should provide the following information to the cloud consumer in relation with provision of information on information security incidents: <ul style="list-style-type: none"> a) reporting channel; b) person or organization in charge of reporting; c) criteria for information security incident at cloud provider. <i>[JP67]</i>

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 Consumer	Cloud Provider
Cloud consumer should develop criteria and procedure to inform providers about information security events. Cloud consumer should request cloud provider to report information security events which could affect cloud consumer's environment to respond those events. Cloud consumer should request information to the cloud provider to develop criteria and	Cloud provider should provide the following information to the cloud consumer to support the cloud consumer in developing criteria and procedure to receive information about information security events: <ul style="list-style-type: none"> a) contacts; b) contact method. Cloud provider should provide the following

procedure to inform providers about information security events. [JP68]	<p>information to the cloud consumer to support cloud consumer in handling information security events:</p> <ul style="list-style-type: none"> a) reporting channel; b) person or organization in charge of reporting; c) criteria for information security event report. d) reporting data format. [JP69] e) historical availability of services going back 1 year, including a clear definition of what constitutes an “available” service f) Security investigations underway and average response time and duration of investigations g) Rate and frequency of external denial of service attacks, both brute force and protocol-based (low and slow) attacks h) Rate and frequency of virus or malware detection within the service provider infrastructure i) Change logs [CA11] j) request commitment to maximum or average response time [CSA32] k) request incident severity level according to an agreed classification scheme [CSA32]
---	---

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. The following sector-specific guidance also applies.

Cloud Consumer	Cloud Provider
Cloud consumer should develop criteria and procedure to inform providers about security weaknesses.	Cloud provider should provide the following information to the cloud consumer to support the cloud consumer in developing criteria and procedure to inform providers about information security weaknesses:
Cloud consumer should request information to the cloud provider to develop criteria and procedure to inform providers about security weakness. [JP70]	<ul style="list-style-type: none"> a) contacts; b) contact method.
Cloud consumer should request information to the cloud provider to have report of security weaknesses. [JP70]	Cloud provider should provide the following information to support the cloud consumer in having report on information security

	<p>weaknesses:</p> <p>a) reporting channel;</p> <p>b) person or organization in charge of reporting;</p> <p>c) criteria of issuing security weaknesses report. [JP71]</p>
--	---

16.1.4 Assessment and decision of information security events

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

16.1.5 Response to information security incidents

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

16.1.6 Learning from information security incidents

Control 16.1.6 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud Consumer	Cloud Provider
<p>Cloud consumer should include incidents of cloud service into a process of information security incidents evaluation using the following information. [US82]</p> <p>a) statistics of information security incident;</p> <p>b) effect by information security incident;</p> <p>c) response to information security incident;</p> <p>d) preventive action of information security incident.</p> <p>Cloud consumer should request cloud provider to provide result of information security incident evaluation. Cloud consumer should request the following information to the cloud provider to evaluate information security incidents. [JP72]</p>	<p>Cloud provider should provide the following information to the cloud consumer to evaluate information security incidents:</p> <p>a) statistics of information security incident;</p> <p>b) effect by information security incident;</p> <p>c) response to information security incident;</p> <p>d) preventive action of information security incident. [JP73]</p>

16.1.7 Collection of evidence

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

Cloud Consumer	Cloud Provider
<p>Cloud consumer should do the followings when cloud provider manages information which might be legal evidence at cloud consumer:</p> <ul style="list-style-type: none"> a) identify information which might be legal evidence at the own organization; b) confirm if information managed by cloud provider is recorded and properly stored; c) collect and retain information managed by cloud provider; d) identify what constitutes valid evidence for the cloud consumer. <p>Cloud consumer should request information to cloud provider, when cloud provider manages the information that might be legal evidence for cloud consumer: <i>[JP74]</i></p>	<p>Cloud provider should provide the following information to the cloud consumer, when cloud provider manages the information that can be legal evidence for cloud consumer:</p> <ul style="list-style-type: none"> a) affordable items and scope; b) retention method (from legal point of view); c) retention period; d) affordable period; e) billing information: <ul style="list-style-type: none"> 1) procedure; 2) cost; 3) delivery time.<i>[JP75]</i> f) Description of process for forensic support g) available information (from VMs, network, SIEM, offline VMs, IPS and other sources) h) Interfaces and APIs forensic information will be provided through i) protection measures against collateral damage during a forensic investigation on shared resources j) protection of sensitive information from other tenants during a forensic investigation on shared resources like RAM or Network k) Skills of available employees supporting forensic investigations l) provider awareness of local laws m) Procedures and measures to strictly isolate customer related evidence data <i>[CSA34]</i> <p>Cloud provider should consider data protection constraints and best practices in dealing on data retention.</p>

17 Information security aspects of business continuity management

17.1 Information security continuity

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

17.1.1 Planning information security continuity

Control 17.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud Consumer	Cloud Provider
Cloud consumer should assess risk of business continuity with cloud service use. Cloud consumer should request information to the cloud provider related to the risks of cloud service that affect business continuity as a part of risk assessment: <i>[JP76]</i>	Cloud provider should provide information related to the following risks related to the cloud consumer's business continuity to the cloud consumer to support risk assessment: <ul style="list-style-type: none"> a) Failure of cloud service; b) Internet connectivity reliability between cloud consumer and cloud provider; <i>[CSA35]</i> c) Service unavailability by law enforcers' confiscation; d) Termination of cloud service; e) Change in ownership and statements indicating financial stability <i>[JP77]</i>

17.1.2 Implementing information security continuity

Control 17.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud Consumer	Cloud Provider
Cloud consumer should define requirements for business continuity with cloud service. Cloud consumer should develop and implement business continuity plan including cloud service. Cloud consumer should request information to the cloud provider to develop and implement business continuity plan covering cloud service. <i>[JP78]</i>	Cloud provider should provide the following information to the cloud consumer to develop and implement business continuity plan covering cloud service: <ul style="list-style-type: none"> a) disaster recovery plan; b) availability ensuring measure such as system duplication. <i>[JP79]</i>

17.1.3 Verify, review and evaluate information security continuity

Control 17.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud Consumer	Cloud Provider
<p>Cloud consumer should define requirements for business continuity with cloud service. Cloud consumer should develop and implement business continuity plan including cloud service. Cloud consumer should request information to the cloud provider to develop and implement business continuity plan covering cloud service. [JP78]</p> <p>Cloud consumer should involve cloud provider to test and update business continuity plan. Cloud consumer should ensure that appropriate terms of service availability provisions are agreed upon that can be incorporated in the testing and updating of applicable cloud consumer business continuity plans. [CSA36]</p>	<p>Cloud provider should provide the following information to the cloud consumer to develop and implement business continuity plan covering cloud service:</p> <ul style="list-style-type: none"> a) disaster recovery plan; b) availability ensuring measure such as system duplication. [JP79] <p>Cloud provider should provide information on its availability to be involved in testing and updating cloud consumer's business continuity plan. [JP80]</p>

17.2 Redundancies

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

17.2.1 Availability of information processing facilities

Control 17.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud Consumer	Cloud Provider

[Editor's note: US NB is requested to provide contributions for US43 comment in Rome editing meeting.]

18 Compliance

18.1 Information security reviews

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

18.1.1 Independent review of information security

Control 18.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

18.1.2 Compliance with security policies and standards

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

18.1.3 Technical compliance inspection

Control 18.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud Consumer	Cloud Provider
Cloud consumer should define the requirements to confirm that the technical compliance checking of cloud services be implemented by cloud provider. Cloud consumer should confirm that the technical compliance checking of cloud services be implemented by cloud provider. Cloud consumer should request information on the provider's compliance checking method of cloud service to confirm that the technical compliance checking is implemented. <i>[JP87]</i>	Cloud provider should provide the following information on the compliance checking method of cloud service to the cloud consumer to show the technical compliance checking is implemented: a) objects; b) methods; c) frequency; d) results; e) corrective action for non-compliances <i>[JP88]</i>

18.2 Compliance with legal and contractual requirements

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

18.2.1 Identification of applicable legislation and contractual requirements

Control 18.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud Consumer	Cloud Provider
----------------	----------------

Cloud consumer should identify domestic and foreign legal, regulatory and contractual requirements depending on purpose of cloud service use.	Cloud provider should provide information on legal and regulatory requirements of the country or region from where the cloud service is provided. [JP82] Where cloud provider uses upstream cloud services, their jurisdictions and applicable laws and regulations should be identified documented and kept up to date by the cloud provider. [JP81] Cloud provider should monitor for compliance to ensure customer data is contained within applicable geo-location or legislative jurisdictional restrictions. [CSA37]
---	---

18.2.2 Intellectual property rights (IPR)

Control 18.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud Consumer	Cloud Provider
Cloud consumer should identify requirements on intellectual property depending on purpose of cloud service use.	Cloud provider should provide information to the cloud consumer on intellectual property rights which cloud provider claims to own. [JP83]

18.2.3 Protection of documented information

Control 18.2.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud Consumer	Cloud Provider
Cloud consumer should confirm if cloud provider can retain important records on cloud service for regulated period. Cloud consumer should request information on retention of records to the cloud provider to confirm that cloud provider can retain records for regulated period when cloud consumer handles important records with legal and regulatory requirements on the cloud service. [JP84]	Cloud provider should provide the following information to the cloud consumer to confirm that cloud provider can retain records for regulated period when cloud consumer handle important records with legal and regulatory requirements: a) applicable laws and regulations; b) retention method; c) retention period. [JP85]

18.2.4 Privacy and protection of personally identifiable information

Control 18.2.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud Consumer	Cloud Provider
Cloud consumer should identify domestic and foreign legal, regulatory and contractual requirements of data protection and privacy of personal information depending on purpose of cloud service use. Cloud consumer should request information on domestic and foreign legal and regulatory requirements of data protection and privacy of personal information to the cloud provider to clarify legal and regulatory requirements of the country or region from where cloud service is provided. <i>[CSA38]</i>	Cloud provider should provide information on legal jurisdiction which affects cloud service to the cloud consumer to support it identifying relevant legislation to data protection and privacy of personal information. Cloud provider should provide information on domestic and foreign legal and regulatory requirements of data protection and privacy of personal information applicable to the cloud service to the cloud consumer. <i>[JP86]</i>

18.2.5 Regulation of cryptographic controls

Control 18.2.5 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud Consumer
Cloud consumer should confirm that cryptographic technology used is not conflict with regulations on export in provided country or region.

Annex A: Cloud Computing Service Extended Control Set (Normative)

This Annex provides definitions for new objectives, new controls and new implementation guidance, as a cloud computing service extended control set. ISO/IEC 27002 control objectives related to this 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. *[WD2:DoC US21].*

[WD2:DoC US22. Specific cloud computing code “CLD”]

CLD.6 Organization of information security

CLD.6.1 Internal organization

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

CLD.6.1.8 Management commitment to information security

[Editor’s note: Either case of the following two cases must be applied. This decision has been postponed to the next meeting according to the resolution of Rome 27017 editing meeting. For more details, see Major issue 11 of 27017 meeting report (N12017).]

Case1: To move the regarding cloud specific implementation guidance to the appropriate control of WD4 27017 main body

Case2: To create “new” additional cloud specific control objective and controls, and put the regarding cloud specific implementation guidance into the regarding “new” additional cloud specific controls

Implementation guidance for cloud consumer

Management should approve the company information security policy and provide resources to implement and maintain information security programs and controls across the organization

Management should approve assignment of specific roles and responsibilities for information security across the organization relevant to the use of cloud service. *[WD1:DoC CA10]*

Implementation guidance for cloud provider

Security policy changes with material operational impact should require formal notification of subcontractors, tenants, supporting service tiers and employees of the impact and ramifications.

Executive and line management should take formal action to support information security through clear documented direction, commitment, explicit assignment and verification of assignment execution. *[WD1:DoC US10, CA9]*

Other Information

Further information is contained in ISO/IEC 13335-1:2004.

CLD.6.1.9 Information security co-ordination

[Editor's note: Either case of the following two cases must be applied. This decision has been postponed to the next meeting according to the resolution of Rome 27017 editing meeting. For more details, see Major issue 11 of 27017 meeting report (N12017).]

Case1: To move the regarding cloud specific implementation guidance to the appropriate control of WD4 27002 main body

Case2: To create “new” additional cloud specific control objective and controls, and put the regarding cloud specific implementation guidance into the regarding “new” additional cloud specific controls

Implementation guidance for cloud consumer

Information security education, training and awareness about cloud service should be provided to management and the supervising managers including those of business units as part of information security co-ordination to co-ordinate information security activities effectively.

Cloud consumer should provide opportunities to share and exchange information about use of cloud service.

Implementation guidance for cloud provider

[Editor's note: The following three lines are moved from “Requests to cloud service providers” to “Implementation guidance for cloud provider”. NBs and liaisons are requested to provide contributions to fit to the text in “Implementation guidance for cloud provider”.]

Cloud consumer should request cloud provider to offer user manuals, precautions and contacts regarding the cloud service for the purpose of information security education, training, and awareness programme of cloud service.

Where applicable, the cloud provider should issue user manuals, precautions, and contacts regarding the cloud service for the purpose of IS education, training and awareness programme of cloud service.

[WD1:DoC CA11]

CLD.6.2 External parties

CLD.6.2.1 Identification of risks related to external parties

[Editor's note: Either case of the following two cases must be applied. This decision has been postponed to the next meeting according to the resolution of Rome 27017 editing meeting. For more details, see Major issue 11 of 27017 meeting report (N12017).]

Case1: To move the regarding cloud specific implementation guidance to the appropriate control of WD4 27002 main body

Case2: To create “new” additional cloud specific control objective and controls, and put the regarding cloud specific implementation guidance into the regarding “new” additional cloud specific controls

Implementation guidance for cloud consumer

Cloud consumer should identify the risks to the cloud consumer's information and information process facilities caused by the use of cloud service and implement appropriate controls before starting to use the services.

The identification of risks specific to cloud service should take into account that:

- a) the information is stored in the hardware owned by cloud provider;
- b) cloud provider may use other cloud service;
- c) business processes of other cloud consumer may share the same hardware;
- d) after the termination of use of the cloud service, the system resource used by the services is generally being reused;
- e) information security policy and information security implementation which would not be effective upon use of cloud service. some part of information security policy and controls may be ineffective upon use of cloud service;
- f) changes in operating environment like mobility etc. that can be achieved by using cloud service. Business operation, e.g. mobile computing, may change by the use of cloud service.
- g) legal restriction and/or inability of the cloud provider to allow access to information due to risk of exposures of information of other cloud consumer organization . [WD1:DoC CA17]
- h) jurisdiction, legal and regulatory requirements and other contractual obligations relevant to the external party that should be taken into account; [WD1:DoC CA18]
- i) legal and regulatory differences between the cloud consumer information assets and the cloud provider service-delivery assets. [WD1:DoC CA19]

Annex E provides examples of risk sources specific to cloud computing and cloud service.

Implementation guidance for cloud provider

[Editor's note: The following twenty lines are moved from "Requests to cloud service providers" to "Implementation guidance for cloud provider". NBs and liaisons are requested to provide contributions to fit to the text in "Implementation guidance for cloud provider".]

[WD1:DoC CA20]

Cloud consumer should request the following information to the cloud provider to identify risks of cloud service:

- a) use of cloud computing sub-services;
- b) agreement including service level agreement and non-disclosure agreement;
- c) information security audit report covering; Security controls implemented by the cloud provider, such as :
 - 1) organization of information security;
 - 2) asset management;
 - 3) human resources security;
 - 4) physical and environmental security;
 - 5) access control;
 - 6) information systems acquisition, development and maintenance;
 - 7) information security incident management;
 - 8) business continuity management;;
- d) acceptance level of cloud provider for specific security control request by cloud consumer;
- e) applicable jurisdiction. (need to be more descriptive).
- f) applicable jurisdiction of all cloud infrastructures managing cloud consumer information under both normal and abnormal circumstances. [WD1:DoC CA21]

Where external party requires access to the cloud provider facilities or information of a particular cloud consumer organization, a risk assessment (see also ISO/IEC 27001 and ISO/IEC 27005) should be carried out to identify any requirements for specific controls. The external party should also have proper authorization from the cloud consumer organization whose information will be accessed. (*WD1:DoC CA16*).

Other Information

Information might be put at risk by external parties with inadequate security management. Controls should be identified and applied to administer external party access to information processing facilities. For example, if there is a special need for confidentiality of the information, non-disclosure agreements might be used.

Organizations may face risks associated with inter-organizational processes, management, and communication if a high degree of outsourcing is applied, or where there are several external parties involved.

The controls 6.2.2 and 6.2.3 cover different external party arrangements, e.g. including:

- a) service providers, such as ISPs, network providers, telephone services, maintenance and support services;
- b) managed security services;
- c) customers;
- d) outsourcing of facilities and/or operations, e.g. IT systems, data collection services, call centre operations;
- e) management and business consultants, and auditors;
- f) developers and suppliers, e.g. of software products and IT systems;
- g) cleaning, catering, and other outsourced support services;
- h) temporary personnel, student placement, and other casual short-term appointments.

Such agreements can help to reduce the risks associated with external parties.

Other information for cloud computing

Cloud consumer should be aware that the information regarding the information security control disclosed by cloud provider can be limited or abstract in many cases, because security and risk disclosures may represent sensitive information related to other cloud consumers of the same cloud provider. [*WD1:DoC CA22*]

CLD.6.2.2 Addressing Security when dealing with customers

[Editor's note: Either case of the following two cases must be applied. This decision has been postponed to the next meeting according to the resolution of Rome 27017 editing meeting. For more details, see Major issue 11 of 27017 meeting report (N12017).]

Case1: To move the regarding cloud specific implementation guidance to the appropriate control of WD4 27002 main body

Case2: To create “new” additional cloud specific control objective and controls, and put the regarding cloud specific implementation guidance into the regarding “new” additional cloud specific controls

Implementation guidance for cloud consumer

Cloud consumer should identify the additional works and risks of its customers related to using cloud service.

Cloud consumer should specify vulnerabilities and threats that affect not only itself but also its customers.

Prior to granting customers access to data, assets and information systems, all identified security, contractual and regulatory requirements for customer access should be addressed and remediated.

[WD1:DoC CA23]

The cloud consumer should be responsible for reporting the internal controls of its services to its customers. cloud consumer can obtain information security report audit report of the cloud provider to support its internal controls reporting to its customers.

The cloud consumer should inform its customers that the access to information in the cloud services may be legally restricted in accordance to privacy laws and that the cloud provider may not be allowed to grant access to information without the risk of exposing information of other cloud consumer organization .

[WD1:DoC US11]

Classification needs to implemented, understood and applied throughout the supply chain.

Other information for cloud computing

The examples to be identified that the customer of cloud consumer can be affected by the use of cloud service are as follows:

- a) the level of the service that cloud consumer provides for its customer depends on the service level of cloud service used;
- b) the jurisdiction of the country in where the information processing facilities for the cloud service are located;
- c) the cloud service which are provided from the same/nearby location where its customer has backup for the their business continuity.

CLD.6.2.3 Addressing security in third party agreements

[Editor's note: Either case of the following two cases must be applied. This decision has been postponed to the next meeting according to the resolution of Rome 27017 editing meeting. For more details, see Major issue 11 of 27017 meeting report (N12017).]

Case1: To move the regarding cloud specific implementation guidance to the appropriate control of WD4 27002 main body

Case2: To create “new” additional cloud specific control objective and controls, and put the regarding cloud specific implementation guidance into the regarding “new” additional cloud specific controls

Implementation guidance for cloud consumer

Cloud consumer should identify the security requirements for cloud service based on its security risk assessment. *[WD1:DoC CA24]*

Cloud consumer should ensure that the agreement satisfy the security requirements.

The comparison between the security requirements and the agreement should be approved by management or appropriate responsible manager.

[WD1:DoC US11]

Classification needs to be implemented, understood and applied throughout the supply chain.

Implementation guidance for cloud provider

[Editor's note: The following fourteen lines are moved from "Requests to cloud service providers" to "Implementation guidance for cloud provider". NBs and liaisons are requested to provide contributions to fit to the text in "Implementation guidance for cloud provider".]

Cloud consumer should request cloud provider the following information to judge if the cloud service satisfies own information security requirements (see 6.1.3):

- a) service agreement, for example:
 - 1) security control;
 - 2) service definition;
 - 3) service level;
 - 4) statement of security conformity across all cloud provider data centres *[WD1:DoC CA25]*
- b) premises to keep the agreement, for example:
 - 1) responsible person;
 - 2) organization functions/structure;
 - 3) security management standard;
- c) premises to keep the service level agreements, for example:
 - 1) inspection report;
 - 2) audit report.

CLD.11 Communications and Operations

CLD.11.1 Operational procedures and responsibilities

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

CLD.11.1.5 System acceptance

[Editor's note: Either case of the following two cases must be applied. This decision has been postponed to the next meeting according to the resolution of Rome 27017 editing meeting. For more details, see Major issue 11 of 27017 meeting report (N12017).]

Case1: To move the regarding cloud specific implementation guidance to the appropriate control of WD4 27002 main body

Case2: To create "new" additional cloud specific control objective and controls, and put the regarding cloud specific implementation guidance into the regarding "new" additional cloud specific controls

Implementation guidance for cloud consumer

Cloud consumer should establish acceptance criteria of cloud service (see 6.1.2).

Cloud consumer should carry out adequate system testing prior to acceptance of cloud service.

Implementation guidance for cloud provider

[Editor's note: The following five lines are moved from "Requests to cloud service providers" to "Implementation guidance for cloud provider". NBs and liaisons are requested to provide contributions to fit to the text in "Implementation guidance for cloud provider".]

Cloud consumer should request the following information to the cloud provider to select a cloud service:

- a) service level agreement, including access-network capacity and redundancy (see CLD.6.2.3); [WD1:DoC CA32]
- b) trial use specifications, including fees, trial period and disclaimer.

CLD.11.2 Protection from malware

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

CLD.11.2.2 Controls against unauthorized mobile code

[Editor's note: Either case of the following two cases must be applied. This decision has been postponed to the next meeting according to the resolution of Rome 27017 editing meeting. For more details, see Major issue 11 of 27017 meeting report (N12017).]

Case1: To move the regarding cloud specific implementation guidance to the appropriate control of WD4 27002 main body

Case2: To create "new" additional cloud specific control objective and controls, and put the regarding cloud specific implementation guidance into the regarding "new" additional cloud specific controls

Implementation guidance for cloud consumer

Cloud consumer should identify mobile codes used in the cloud service, and define procedure to restrict their usage if needed.

Implementation guidance for cloud provider

[Editor's note: The following four lines are moved from "Requests to cloud service providers" to "Implementation guidance for cloud provider". NBs and liaisons are requested to provide contributions to fit to the text in "Implementation guidance for cloud provider".]

Cloud consumer should request the following information to the cloud provider to confirm controls on mobile codes usage:

- a) services using mobile codes;
- b) mobile codes in use.

Other information for cloud computing

Some of the examples of mobile code are embedded script. Since mobile code is associated with a number of middleware services, controls for middleware may be considered in addition to general controls for malicious code.

CLD.11.8 Logging and Monitoring

The objective specified in clause 11.8 of ISO/IEC 27002 applies.

CLD.11.8.6 Audit logging

[Editor's note: Either case of the following two cases must be applied. This decision has been postponed to the next meeting according to the resolution of Rome 27017 editing meeting. For more details, see Major issue 11 of 27017 meeting report (N12017).]

Case1: To move the regarding cloud specific implementation guidance to the appropriate control of WD4 27002 main body

Case2: To create “new” additional cloud specific control objective and controls, and put the regarding cloud specific implementation guidance into the regarding “new” additional cloud specific controls

Implementation guidance for cloud consumer

Cloud consumer should develop a policy on the use of cloud service functions and own development to record audit logs of user activities, exception handling and information security events.

Implementation guidance for cloud provider

[Editor's note: The following seven lines are moved from “Requests to cloud service providers” to “Implementation guidance for cloud provider”. NBs and liaisons are requested to provide contributions to fit to the text in “Implementation guidance for cloud provider”.]

Cloud consumer should request the following specifications to the cloud provider to develop a policy and procedures to record audit logs:

- a) events to be logged;
- b) information and data format to be recorded as audit logs;
- c) retention period of audit logs;
- d) interactively accessible period;
- e) method of verifying integrity of audit logs.

Other information for cloud computing

Appropriate measures to ensure non-disclosure of communications should be taken Monitoring system use

Depending on the nature of the cloud service, the audit logs may contain intrusive and confidential personal data. Appropriate privacy protection measures should be taken (see also 17.1.4). Where possible, system administrators should not have permission to erase or de-activate logs of their own activities (see 11.8.3). *[WD1:DoC CA39]*

CLD.13 Access control

CLD.13.4 System and application access control

The objective specified in clause 13.4 of ISO/IEC 27002 applies.

CLD.13.4.5 Sensitive System Isolation

[Editor's note: Either case of the following two cases must be applied. This decision has been postponed to the next meeting according to the resolution of Rome 27017 editing meeting. For more details, see Major issue 11 of 27017 meeting report (N12017).]

Case1: To move the regarding cloud specific implementation guidance to the appropriate control of WD4 27002 main body

Case2: To create “new” additional cloud specific control objective and controls, and put the regarding cloud specific implementation guidance into the regarding “new” additional cloud specific controls

Implementation guidance for cloud consumer

Cloud consumer should confirm that sensitive systems can be developed on a dedicated (isolated) cloud computing environment when they are implemented using cloud service.

Implementation guidance for cloud provider

[Editor's note: The following three lines are moved from “Requests to cloud service providers” to “Implementation guidance for cloud provider”. NBs and liaisons are requested to provide contributions to fit to the text in “Implementation guidance for cloud provider”.]

Cloud consumer should request the specifications of dedicated (isolated) environment to the cloud provider to confirm to develop the sensitive systems on a dedicated (isolated) cloud computing environment.

CLD.13.5 Network access control

CLD.13.5.1 User authentication for cloud service connection

[Editor's note: Either case of the following two cases must be applied. This decision has been postponed to the next meeting according to the resolution of Rome 27017 editing meeting. For more details, see Major issue 11 of 27017 meeting report (N12017).]

Case1: To move the regarding cloud specific implementation guidance to the appropriate control of WD4 27002 main body

Case2: To create “new” additional cloud specific control objective and controls, and put the regarding cloud specific implementation guidance into the regarding “new” additional cloud specific controls

Implementation guidance for cloud consumer

Cloud consumer should use appropriate authentication methods when accessing a cloud service via a network that is outside the control of the organization's security management, e.g. the Internet, public wireless networks or mobile telephone networks. *[WD1:DoC CA45]*.

Implementation guidance for cloud provider

[Editor's note: The following four lines are moved from “Requests to cloud service providers” to “Implementation guidance for cloud provider”. NBs and liaisons are requested to provide contributions to fit to the text in “Implementation guidance for cloud provider”.]

Cloud consumer should request the following information to the cloud provider to authenticate remote users

- a) functional specification to identify the origin of connecting to cloud service;
- b) functional specification to restrict connection to cloud service.

CLD.13.5.2 Equipment Identification in Cloud Networks

[Editor's note: Either case of the following two cases must be applied. This decision has been postponed to the next meeting according to the resolution of Rome 27017 editing meeting. For more details, see Major issue 11 of 27017 meeting report (N12017).]

Case1: To move the regarding cloud specific implementation guidance to the appropriate control of WD4 27002 main body

Case2: To create “new” additional cloud specific control objective and controls, and put the regarding cloud specific implementation guidance into the regarding “new” additional cloud specific controls

Implementation guidance for cloud consumer

Cloud consumer should identify and treat connection from equipment that is using the cloud services from outside the cloud consumer's security management.

Implementation guidance for cloud provider

[Editor's note: The following four lines are moved from “Requests to cloud service providers” to “Implementation guidance for cloud provider”. NBs and liaisons are requested to provide contributions to fit to the text in “Implementation guidance for cloud provider”.]

Cloud consumer should request the following information to the cloud provider to identity equipment connecting remotely:

- a) functional specification to identify equipment connecting to cloud service;
- b) functional specification to restrict connection to cloud service.

CLD.13.5.3 Network Connection Controls

[Editor's note: Either case of the following two cases must be applied. This decision has been postponed to the next meeting according to the resolution of Rome 27017 editing meeting. For more details, see Major issue 11 of 27017 meeting report (N12017).]

Case1: To move the regarding cloud specific implementation guidance to the appropriate control of WD4 27002 main body

Case2: To create “new” additional cloud specific control objective and controls, and put the regarding cloud specific implementation guidance into the regarding “new” additional cloud specific controls

Implementation guidance for cloud consumer

Cloud consumer should restrict the network connection capability so that only authorized cloud consumers can use services allowed among ones offered on cloud service.

For shared networks, especially those extending across the organization's boundaries, the capability of cloud consumers to connect to the network should be restricted, in line with the access control policy and requirements of the business application and legislative jurisdiction. [WD1:DoC US32].

Implementation guidance for cloud provider

[Editor's note: The following four lines are moved from "Requests to cloud service providers" to "Implementation guidance for cloud provider". NBs and liaisons are requested to provide contributions to fit to the text in "Implementation guidance for cloud provider".]

Cloud consumer should request the following information to the cloud provider to restrict the capability to connect to the network of cloud service:

- a) functional specification to restrict the network connection;
- b) information usable to restrict the network connection capability.

CLD.13.5.4 Network routing control

[Editor's note: Either case of the following two cases must be applied. This decision has been postponed to the next meeting according to the resolution of Rome 27017 editing meeting. For more details, see Major issue 11 of 27017 meeting report (N12017).]

Case1: To move the regarding cloud specific implementation guidance to the appropriate control of WD4 27002 main body

Case2: To create "new" additional cloud specific control objective and controls, and put the regarding cloud specific implementation guidance into the regarding "new" additional cloud specific controls

Control

Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.

Implementation guidance

Routing controls should be based on positive source and destination address checking mechanisms. Security gateways can be used to validate source and destination addresses at internal and external network control points if proxy and/or network address translation technologies are employed.

Implementers should be aware of the strength and shortcomings of any mechanisms deployed. The requirements for network routing control should be based on the access control policy (see 13.1).

Routing controls should be implemented to ensure that computer connections and information flows do not breach the access control policy of the business applications or the policies associated with jurisdictional regulations. Mechanisms should be put in place to enforce routing constraints based on legal jurisdiction. [WD1:DoC US33]

Other information

Shared networks, especially those extending across organizational boundaries, may require additional routing controls. This particularly applies where networks are shared with third party (nonorganization) users.

CLD.13.6 Operating system access control

CLD.13.6.1 User identification and authentication

[Editor's note: Either case of the following two cases must be applied. This decision has been postponed to the next meeting according to the resolution of Rome 27017 editing meeting. For more details, see Major issue 11 of 27017 meeting report (N12017).]

Case1: To move the regarding cloud specific implementation guidance to the appropriate control of WD4 27002 main body

Case2: To create “new” additional cloud specific control objective and controls, and put the regarding cloud specific implementation guidance into the regarding “new” additional cloud specific controls

Implementation guidance for cloud consumer

Cloud consumer should confirm that all cloud consumers can have a unique identifier (user ID) for their personal use only.

Cloud consumer should confirm that a suitable authentication technique can be used in cloud service to substantiate the claimed identity of a user.

Implementation guidance for cloud provider

[Editor's note: The following two lines are moved from “Requests to cloud service providers” to “Implementation guidance for cloud provider”. NBs and liaisons are requested to provide contributions to fit to the text in “Implementation guidance for cloud provider”.]

Cloud consumer should request the detailed functional specifications of user authentication to the cloud provider to confirm appropriate authentication technique is used.

CLD.13.6.2 Session time-out

[Editor's note: Either case of the following two cases must be applied. This decision has been postponed to the next meeting according to the resolution of Rome 27017 editing meeting. For more details, see Major issue 11 of 27017 meeting report (N12017).]

Case1: To move the regarding cloud specific implementation guidance to the appropriate control of WD4 27002 main body

Case2: To create “new” additional cloud specific control objective and controls, and put the regarding cloud specific implementation guidance into the regarding “new” additional cloud specific controls

Implementation guidance for cloud consumer

Cloud consumer should confirm that inactive sessions are shut down after a defined period of inactivity when using cloud service.

Implementation guidance for cloud provider

[Editor's note: The following six lines are moved from "Requests to cloud service providers" to "Implementation guidance for cloud provider". NBs and liaisons are requested to provide contributions to fit to the text in "Implementation guidance for cloud provider".]

Cloud consumer should request the following information to the cloud provider to confirm that inactive sessions are shut down after a defined period of inactivity when using cloud service:

- a) functional specifications to shut down inactive sessions after a defined period of inactivity;
- b) functional specifications to select a period of inactivity to shut down inactive sessions;

CLD.13.6.3 Limitation of connection time

[Editor's note: Either case of the following two cases must be applied. This decision has been postponed to the next meeting according to the resolution of Rome 27017 editing meeting. For more details, see Major issue 11 of 27017 meeting report (N12017).]

Case1: To move the regarding cloud specific implementation guidance to the appropriate control of WD4 27002 main body

Case2: To create "new" additional cloud specific control objective and controls, and put the regarding cloud specific implementation guidance into the regarding "new" additional cloud specific controls

Implementation guidance for cloud consumer

Cloud consumer should confirm that connection time controls are available on a cloud service which use is evaluated as high-risk.

Implementation guidance for cloud provider

[Editor's note: The following two lines are moved from "Requests to cloud service providers" to "Implementation guidance for cloud provider". NBs and liaisons are requested to provide contributions to fit to the text in "Implementation guidance for cloud provider".]

Cloud consumer should request the information about specifications of the connection time controls to the cloud provider to limit the duration of active sessions.

CLD.14 System acquisition, development and maintenance

CLD.14.5 Correct processing in applications

CLD.14.5.1 Input data validation

[Editor's note: Either case of the following two cases must be applied. This decision has been postponed to the next meeting according to the resolution of Rome 27017 editing meeting. For more details, see Major issue 11 of 27017 meeting report (N12017).]

Case1: To move the regarding cloud specific implementation guidance to the appropriate control of WD4 27002 main body

Case2: To create “new” additional cloud specific control objective and controls, and put the regarding cloud specific implementation guidance into the regarding “new” additional cloud specific controls

Implementation guidance for cloud consumer

Cloud consumer should define criteria of validation check of input data to request to cloud service.

Cloud consumer should confirm that the specifications on validation check for input data are adequate to the criteria.

Implementation guidance for cloud provider

[Editor’s note: The following seven lines are moved from “Requests to cloud service providers” to “Implementation guidance for cloud provider”. NBs and liaisons are requested to provide contributions to fit to the text in “Implementation guidance for cloud provider”.]

Cloud consumer should request the following information on validation check to the cloud provider to confirm that the specifications on validation check for input data are adequate to the criteria:

- a) object;
- b) aspects;
- c) permissible range;
- d) response to invalid data.

CLD.14.5.2 Control of internal processing

[Editor’s note: Either case of the following two cases must be applied. This decision has been postponed to the next meeting according to the resolution of Rome 27017 editing meeting. For more details, see Major issue 11 of 27017 meeting report (N12017).]

Case1: To move the regarding cloud specific implementation guidance to the appropriate control of WD4 27002 main body

Case2: To create “new” additional cloud specific control objective and controls, and put the regarding cloud specific implementation guidance into the regarding “new” additional cloud specific controls

Implementation guidance for cloud consumer

Cloud consumer should define criteria of validation check of internal processing to request to cloud service.

Cloud consumer should confirm that the specifications on validation check of internal processing are adequate to the criteria.

Implementation guidance for cloud provider

[Editor's note: The following six lines are moved from "Requests to cloud service providers" to "Implementation guidance for cloud provider". NBs and liaisons are requested to provide contributions to fit to the text in "Implementation guidance for cloud provider".]

Cloud consumer should request the following information on validation check to the cloud provider to confirm that the specifications on validation check of internal processing are adequate to the criteria:

- a) object;
- b) aspects;
- c) response to invalid processing.

CLD.14.5.3 Message integrity

[Editor's note: Either case of the following two cases must be applied. This decision has been postponed to the next meeting according to the resolution of Rome 27017 editing meeting. For more details, see Major issue 11 of 27017 meeting report (N12017).]

Case1: To move the regarding cloud specific implementation guidance to the appropriate control of WD4 27002 main body

Case2: To create "new" additional cloud specific control objective and controls, and put the regarding cloud specific implementation guidance into the regarding "new" additional cloud specific controls

Implementation guidance for cloud consumer

Cloud consumer should define criteria of validation check of message integrity to request to cloud service.

Cloud consumer should confirm that the specifications on validation check of message integrity are adequate to the criteria.

Implementation guidance for cloud provider

[Editor's note: The following five lines are moved from "Requests to cloud service providers" to "Implementation guidance for cloud provider". NBs and liaisons are requested to provide contributions to fit to the text in "Implementation guidance for cloud provider".]

Cloud consumer should request the following information on validation check to the cloud provider to confirm that the specifications on validation check of message integrity are adequate to the criteria:

- a) object;
- b) method.

CLD.14.5.4 Output data validation

[Editor's note: Either case of the following two cases must be applied. This decision has been postponed to the next meeting according to the resolution of Rome 27017 editing meeting. For more details, see Major issue 11 of 27017 meeting report (N12017).]

Case1: To move the regarding cloud specific implementation guidance to the appropriate control of WD4 27002 main body

Case2: To create “new” additional cloud specific control objective and controls, and put the regarding cloud specific implementation guidance into the regarding “new” additional cloud specific controls

Implementation guidance for cloud consumer

Cloud consumer should define criteria of validation check of output data to request to cloud service.

Cloud consumer should confirm that the specifications on validation check for output data are adequate to the criteria.

Implementation guidance for cloud provider

[Editor’s note: The following seven lines are moved from “Requests to cloud service providers” to “Implementation guidance for cloud provider”. NBs and liaisons are requested to provide contributions to fit to the text in “Implementation guidance for cloud provider”.]

Cloud consumer should request the following information on validation check to the cloud provider to confirm that the specifications on validation check for output data are adequate to the criteria:

- a) object;
- b) aspects;
- c) permissible range;
- d) response to invalid data.

CLD.17 Compliance

CLD.17.1 Compliance with legal and contractual requirements

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

CLD.17.1.7 Non-disclosure of communications

[Editor’s note: Either case of the following two cases must be applied. This decision has been postponed to the next meeting according to the resolution of Rome 27017 editing meeting. For more details, see Major issue 11 of 27017 meeting report (N12017).]

Case1: To move the regarding cloud specific implementation guidance to the appropriate control of WD4 27002 main body

Case2: To create “new” additional cloud specific control objective and controls, and put the regarding cloud specific implementation guidance into the regarding “new” additional cloud specific controls

Control

Non-disclosure of communications being handled by cloud providers should be assured.

Implementation guidance

Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details should be identified, documented and reviewed at planned intervals.

Cloud providers should take account of the following guidelines:

- a) Maintaining cloud computing facilities properly to ensure non-disclosure of communications;
- b) Taking necessary measures to prevent unintended disclosure of other communications during normal use at the point of connection between the cloud consumer's terminal facilities and telecommunication circuits;
- c) taking necessary measures to prevent unauthorized access, destruction or falsification of records and data of cloud consumer stored in cloud computing facilities;
- d) Prohibiting the unauthorized or unlawful utilization by staff of the cloud computing organization of any information related to customer communication;
- e) setting the appropriate retention period of cloud computing data, which is within the time period required for carrying out the purposes for retaining data, and delete them at the end of retention period or at the attainment of the purposes without any delay;
- f) Prohibiting providing the secrets in communications to the third parties, without legal enforcement or the consent of cloud consumer themselves;
- g) Offering the functionality in which cloud consumer can decide on a case-by-case basis whether they send their caller ID or not in the provision of caller ID services;
- h) Prohibiting the provision of caller ID to the third parties, without legal enforcement or the consent of cloud consumer themselves;
- i) Offering cloud service customers a choice as to whether or not to list their telephone numbers or ID related to other services, in the provision of directory assistance services. When cloud consumers request their numbers unlisted, cloud providers should exclude their information from directory assistance services without any delay;
- j) When cloud providers are requested to submit the information relating cloud consumer including non-disclosure of communications, then they need to confirm that the request from law-enforcement agencies or other investigative bodies has gone through a legitimate procedure in accordance with the applicable national laws and regulations and does not conflict with the jurisdiction of origination.

CLD.17.2 Compliance with information security policies and standards, and technical compliance

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

CLD.17.2.3 Monitoring System Use

[Editor's note: Either case of the following two cases must be applied. This decision has been postponed to the next meeting according to the resolution of Rome 27017 editing meeting. For more details, see Major issue 11 of 27017 meeting report (N12017).]

Case1: To move the regarding cloud specific implementation guidance to the appropriate control of WD4 27002 main body

Case2: To create "new" additional cloud specific control objective and controls, and put the regarding cloud specific implementation guidance into the regarding "new" additional cloud specific controls

Implementation guidance for cloud consumer

Cloud consumer should develop procedures for monitoring usage of cloud service as information processing facilities, and review the monitoring records following the procedures.

Implementation guidance for cloud provider

[Editor's note: The following five lines are moved from "Requests to cloud service providers" to "Implementation guidance for cloud provider". NBs and liaisons are requested to provide contributions to fit to the text in "Implementation guidance for cloud provider".]

Cloud consumer should request the following specifications to the cloud provider to develop procedures for monitoring usage of the cloud service:

- a) type of usage records;
- b) method of presentation of usage records;
- c) retention period of usage records.

CLD.17.3 Information systems audit considerations

The objective specified in clause 17.3 of ISO/IEC 27002 applies.

CLD.17.3.2 Protection of information systems audit tools

[Editor's note: Either case of the following two cases must be applied. This decision has been postponed to the next meeting according to the resolution of Rome 27017 editing meeting. For more details, see Major issue 11 of 27017 meeting report (N12017).]

Case1: To move the regarding cloud specific implementation guidance to the appropriate control of WD4 27002 main body

Case2: To create "new" additional cloud specific control objective and controls, and put the regarding cloud specific implementation guidance into the regarding "new" additional cloud specific controls

Control

Access to information systems audit tools should be protected to prevent any possible misuse or compromise.

Implementation guidance

Information systems audit tools, e.g. software or data files, should be separated from development and operational systems and not held in tape libraries or user areas, unless given an appropriate level of additional protection.

Other information

If third parties are involved in an audit, there might be a risk of misuse of audit tools by these third parties, and information being accessed by this third party organization. Controls such as 6.2.1 (to assess the risks) and 9.1.2 (to restrict physical access) can be considered to address this risk, and any consequences, such as immediately changing passwords disclosed to the auditors, should be taken.

CLD.17.3.3 Compliance Independent and Third party Audits

[Editor's note: Either case of the following two cases must be applied. This decision has been postponed to the next meeting according to the resolution of Rome 27017 editing meeting. For more details, see Major issue 11 of 27017 meeting report (N12017).]

Case1: To move the regarding cloud specific implementation guidance to the appropriate control of WD4 27002 main body

Case2: To create “new” additional cloud specific control objective and controls, and put the regarding cloud specific implementation guidance into the regarding “new” additional cloud specific controls

Implementation guidance for cloud provider

Cloud provider should subject themselves to third party audits of all metrics relating to service level agreements. *[WD1:DoC US39]*

Annex B: Controls and Implementation Guidance for cloud consumer and cloud provider

(Informative)

Editor's note: At Nairobi meeting, it was agreed to clarify the responsibility of the cloud service user (CSU) and cloud service provider (CSP) regarding controls and implementation guidance. These are changed to cloud consumer and cloud provider at Stockholm meeting. Therefore, NBs and liaisons are requested to provide mapping lists to specify the relations regarding controls and implementation guidance for cloud consumer and cloud provider.

Annex C: Control Applicability by Service type

(Informative)

Editor's note: At Nairobi meeting, it was agreed to include the following Canadian proposal, which was based on 27002:2005 version. Base 27002 is changed to 27002 revised version, therefore, NBs and liaisons are requested to provide the following based on 27002 revised version.

x	Applicable to cloud provider
NA	Not applicable to cloud provider

	IaaS	PaaS	SaaS
Section 5 – Security Policy			
5.1.1 – Information security policy document	x	x	x
5.1.2 – Review of information security policy	x	x	x
Section 6 – Organization of Information Security			
6.1.1 – Management commitment to Information security	x	x	x
6.1.2 – Information security coordination	x	x	x
6.1.3 – Allocation of Information security responsibilities	x	x	x
6.1.4 – Authorization process for Information security facilities	x	x	x
6.1.5 – Confidentiality Agreements	x	x	x
6.1.6 – Contact with Authorities	x	x	x
6.1.7 – Contact with special interest groups	x	x	x
6.1.8 – Independent review of information security	x	x	x
6.2.1 – Identification of risks related to external parties	x	x	x
6.2.2 – Addressing security when dealing with customers	x	x	x
6.2.3 – Addressing security in third party agreements	x	x	x
Section 7 – Asset Management			
7.1.1 – Inventory of assets	x	x	x
7.1.2 – Ownership of assets	x	x	x
7.1.3 – Acceptable use of assets	x	x	x
7.2.1 – Classification Guidelines	x	x	x
7.2.2 – Information labelling and handling	x	x	x
Section 8 – Human Resources Security			
8.1 – Prior to employment	x	x	x
8.2.1 – Management responsibilities	x	x	x
8.2.2 – Information security awareness	x	x	x

	IaaS	PaaS	SaaS
8.2.3 – Disciplinary Process	x	x	x
8.3.1 – Termination responsibilities	x	x	x
8.3.2 – Return of Assets	x	x	x
8.3.3 – Removal of access rights	x	x	x
Section 9 – Physical and Environmental Security			
9.1.1 – Physical security perimeter	x	x	x
9.1.2 – Physical entry controls	x	x	x
9.1.3 – Securing offices, rooms and facilities	x	x	x
9.1.4 – Protecting against external and environmental risks	x	x	x
9.1.5 – Working in secure areas	x	x	x
9.1.6 – Public access, delivery and loading areas	x	x	x
9.2.1 – Equipment siting and protection	x	x	x
9.2.2 – Supporting utilities	x	x	x
9.2.3 – Cabling security	x	x	x
9.2.4 – Equipment maintenance	x	x	x
9.2.5 – Removal of assets	x	x	x
9.2.6 – Security of equipment and assets off-premises	x	x	x
9.2.7 – Secure disposal or re-use of equipment	x	x	x
Section 10 – Communications and Operations Management			
10.1.1 – Documented Operating procedures	x	x	x
10.1.2 – Change Management	x	x	x
10.1.3 – Segregation of duties	x	x	x
10.1.4 – Separation of development, test and operational environments	x	x	x
10.2.1 – Service delivery	x	x	x
10.2.2 – Monitoring and review of third party services	x	x	x
10.2.3 – Managing changes to third-party services	x	x	x
10.3.1 – Capacity management	x	x	x
10.3.2 – System Acceptance	x	x	x
10.4.1 – Control against malicious software	x	x	x
10.4.2 – Controls against mobile code	NA	NA	x
10.5.1 – Information back-up	x	x	x

	IaaS	PaaS	SaaS
10.6.1 – Network Controls	x	x	x
10.6.2 – Security of network services	x	x	x
10.7 – Media handling	NA	x	x
10.8 – Exchange of information	x	x	x
10.9 – Electronic commerce services	NA	x	x
10.10.1 – Audit logging	x	x	x
10.10.2 – Monitoring of system use	x	x	x
10.10.3 – Protection of log information	x	x	x
10.10.4 – Administrator and operator logs	x	x	x
10.10.5 – Fault logging	x	x	x
10.10.6 – Clock synchronization	x	x	x
Section 11 – Access Control			
11.1 – Access Control policy	NA	x	x
11.2.1 – User registration	NA	x	x
11.2.2 – Privilege management	NA	x	x
11.2.3 – User password management	NA	x	x
11.2.4 – Review of user access rights	NA	x	x
11.3.1 – Password use	NA	x	x
11.3.2 – unattended user equipment	NA	x	x
11.3.3 – Clear desk and screen policy	NA	NA	x
11.4.1 – Policy on use of network services	x	x	x
11.4.2 – User authentication for external connections	NA	NA	x
11.4.3 – Equipment identification in networks	x	x	x
11.4.4 – Remote diagnostics and configuration port protection	NA	x	x
11.4.5 – Segregation of networks	x	x	x
11.4.6 – Network connection control	x	x	x
11.4.7 – Network routing control	x	x	x
11.5.1 – Secure log-on procedures	NA	NA	x
11.5.2 – User identification and authentication	NA	NA	x
11.5.3 – Password management system	NA	x	x
11.5.4 – Use of system utilities	NA	x	x

	IaaS	PaaS	SaaS
11.5.5 – Session time-out	NA	NA	x
11.5.6 – Limitation of connection time	NA	NA	x
11.6.1 – Information access restriction	NA	NA	x
11.6.2 – Sensitive system isolation	NA	x	x
11.7.1 – Mobile computing and communications	NA	NA	x
11.7.2 – Teleworking	NA	NA	x
Section 12 – Information System Acquisition Development and Maintenance			
12.1.1 – Security requirements analysis and specification	x	x	x
12.2.1 – Input data validation	NA	NA	x
12.2.2 – Control of Internal processing	NA	NA	x
12.2.3 – Message integrity	NA	NA	x
12.2.4 – Output data validation	NA	NA	x
12.3.1 – Policy on the use of cryptographic controls	NA	x	x
12.3.2 – Key management	NA	x	x
12.4 – Security of system files	NA	x	x
12.5.1 – Change control procedures	x	x	x
12.5.2 – Technical review of application after operating system changes	NA	x	x
12.5.3 – Restrictions on changes to software packages	x	x	x
12.5.4 – Information leakage	NA	x	x
12.5.5 – Outsourced software development	x	x	x
12.6.1 – Control of technical vulnerabilities	x	x	x
Section 13 – Information Security Incident Management			
13.1.1 – reporting information security events	x	x	x
13.1.2 – reporting security weaknesses	x	x	x
13.2.1 – Responsibility and procedures	x	x	x
13.2.2 – Learning from information security incidents	x	x	x
13.2.3 – collection of evidence	x	x	x
Section 14 – Business Continuity Management			
14.1.1 – Including information security in the business continuity management process	x	x	x
14.1.2 – Business continuity and risk assessment	x	x	x

	IaaS	PaaS	SaaS
14.1.3 – Developing and implementing continuity plans including information security	x	x	x
14.1.4 – Business continuity planning framework	x	x	x
14.1.5 – Testing, maintaining and re-assessing business continuity plans	x	x	x
Section 15 – Compliance			
15.1.1 – Identification of applicable legislation	x	x	x
15.1.2 – Intellectual property rights	x	x	x
15.1.3 – Protection of organizational records	NA	x	x
15.1.4 – Data protection and privacy of personal information	NA	NA	x
15.2.1 – Compliance with security policies and standards	x	x	x
15.2.2 – Technical compliance checking	x	x	x
15.3.1 – Information system audit controls	x	x	x
15.3.2 – Protection of information systems audit tools	x	x	x

Annex D: Risk sources specific to cloud computing and cloud service

(informative)

Editor's note: At Rome meeting, it was agreed that NBs and liaisons are requested to provide the cloud specific risks.

The following are sources of risks of cloud computing and cloud service.

Access control

Some cloud service provide access rights based on the different policy than the one at cloud consumer. And such difference could make access control difficult.

Access point

Rapid growth of public wireless network and/or 3G networks provides access points at various places. And network access from such increased access points at various locations is making network access control difficult.

Application

Some applications provided via SaaS have restricted functionalities. For example, some desktop applications do not reflect all of the items when importing application data from the on-premise version. In addition, applications provided via SaaS do not have enough mutual data compatibilities.

Attack against usage base charge

Depending on contract of cloud service, it charges depending on resource usage. And attack to increase processing level more than originally required could be performed from outside. This kind of attack is performed not to prevent service usage like DoS but to prevent business continuity from the economic standpoint. Some of such attack related to economy is called EDoS (Economic Denial of Sustainability).

Business continuity of cloud provider

When cloud provider got unable to continue their business or decided to stop cloud service, use of the cloud service could be restricted and information on the cloud service could be unavailable, and/or information stored on the cloud service could be lost.

Connectivity

Cloud provider has data centres to provide cloud service at various locations regardless inside or outside of the country, and such data centres are co-working. Due to such environment, there is issue that network structure get complicated and it becomes unable to know reliability of network connection.

Data centre location

From the standpoint of cloud consumer, variability of quality of work caused by different level of experience/moral among the countries where data centre for cloud service is one the concern when adopting cloud service. In addition, difference of network connectivity and so on could cause difference of service quality level. Also, the information on cloud service could be seized based on the jurisdiction of the country where the data centre is located.

Distributed management

Although redundancy and expandability are considered to be benefit of cloud service, management method to have such benefit includes but not limited to distributed management makes information

and system structure complicated, prevents visualization from cloud consumer, and makes centralized management of information and systems difficult.

DoS attack

When DoS attack was made against either cloud provider or cloud consumer, cloud service could be stopped as it is provided via network. In the case of cloud service, it is not possible for cloud consumer to respond as all the equipments to protect/respond to the DoS attack is in the hands of cloud provider.

Encryption

Although many cloud service provide option of encrypted communication by SSL/TLS, some cloud provider does not provide such option and/or does not adopt encryption on their internal network. In such case, the issue that data is not encrypted on the internal network of cloud provider although it is regulated to encrypt when confidential data and/or important data is transferred could be raised.

Helpdesk

Some cloud service from overseas cloud provider may not provide helpdesk service in cloud consumer's language and business hours due to time difference.

ID management

Some cloud service do not provide interfaces to integrate/interfere both of the on-premise ID management and ID management at cloud service. In the case, the systems administration work at cloud consumer could be increased and more complicated to trigger human errors at security management.

Incident management

Cloud consumer could fail to have enough information to respond incident related to cloud service, as cloud consumer can not investigate cloud service to the same level as on-premise systems. Especially when incident management policies/procedures are different between cloud provider and cloud consumer, cloud consumer could fail to respond as defined on their policies/procedures as well as understand its impact.

License management

Cloud consumer could fail to know utilization status of software, since some software license policy/structure does not consider cloud service. For the reason, trouble at software audit could happen.

Log audit

At the cloud service from which log related to network includes access to services, there is issue that cloud consumer cannot respond attack pre-emptively, since it is difficult to know that their asset could be at risk for example when their server is being scanned.

Maintenance utility

Cloud consumer could fail to have enough information at timely bases, since utilities to know status of system is not provided. Such failure of having information makes it unable not only to pre-judge trouble but also to know the status of IT utilization from the standpoint of managements.

Man-In-The-Middle attack

Considering data centres locate various places and co-working, the risk of man-in-the-middle attack is larger than 1-to-1 connection. And service which adopts mash-up is expected to increase the risk even more.

Memory management

It is difficult to investigate trouble caused by memory protection, since physical memory management is not possible at cloud provider; whether hardware, technical problem caused by virtualization and others, and so on.

Mobile phone/smart phone

Since mobile phone and smart phone do not have so many options to enhance security as PC and are not widely adopted yet, there is issue of not enough information related to trouble and response when cloud service is available from mobile phone and smart phone.

MTPD (Maximum Tolerable Period of Disruption)

Clear guideline is required for MTPD of system. MTPD is defined by cloud provider and cloud consumer must wait for recovery as it is defined by cloud provider.

Multitenant

Since multiple cloud consumer share single hardware at some cloud service, attack against such hardware affects all of the cloud consumer sharing the hardware even if they are not intended target of the attack. Especially, in the environment of cloud service, unable to know which cloud consumer is sharing system with which cloud consumer is issue.

Mutual manageability

Since various standardization related to cloud service includes not limited to technology, data format, and service providing style is not completed yet, problem that application data and/or image data of systems generated on a cloud service cannot be used on other cloud service and/or systems cannot co-work could happen.

Physical environment of data centre

From the view point of cloud consumer, there is no significant difference of data centre. But to provide cloud service, data centre with new technologies and new way of implementation includes containers, and un-experienced problem could be caused by such data centre.

Recovery

At cloud service, problem that cloud consumer is unable to notify recovery plan to their customers. Although recovery plan can be notified when it is available based on SLA, it is difficult to notify when it is not the case.

Remaining data

There is issue of being unable to visualize whether remaining data on memory and hard-disk can be controlled efficiently in the virtualized environment.

Restriction of execution environment

Most of the cloud service restrict its execution environment. And some application could not work due to lack of necessary libraries. Since some PaaS vendors provide proprietary development language and visual editor, it makes unable to user service from different cloud provider.

Scale-out technology

Scale-out technology provides benefit of cloud service that high-spec virtual hardware by virtually integrated physical hardware. But since the technology is not tested enough under actual environment, unknown problem could still be hidden.

Systems management and maintenance

It is one of the benefits to adopt cloud service that nearly all of the systems management and maintenance work are transferred to cloud provider. But even in such case from the standpoint of information security, cloud consumer is responsible for systems management and maintenance.

Therefore, to satisfy requirements of cloud consumer's security policy, cloud consumer needs various kind of information.

Virtualization

In the virtualized environment, CPU and memory is managed in different way than physical hardware environment. In addition, virtualized network and/or storage behave differently from physical environment, and it could cause some risk. When application is not designed with considering virtualization, it is expected not only lowered performance but also problem that it does not contribute cost reduction which is original benefit of cloud service due to consuming too much computing resource.

Bibliography

- [1] NIST, SP800-144 *Guidelines on Security and Privacy in Public Cloud Computing*
- [2] NIST, SP800-145 *The NIST Definition of Cloud Computing (Draft)*
- [3] NIST, *Effectively and Securely Using the Cloud Computing Paradigm*
- [4] ENISA, *Cloud Computing Benefits, risks and recommendations for information security*
- [5] ENISA, *Cloud Computing Information Assurance Framework*
- [6] Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1*
- [7] Cloud Security Alliance, *Top Threats to Cloud Computing V1.0*
- [8] Cloud Security Alliance, *Domain 12: Guidance for Identity & Access Management V2.1*
- [9] Cloud Security Alliance, *CSA Cloud Controls Matrix V1.1*
- [10] ISACA, *Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives*
- [11] ISACA, *Cloud Computing Management Audit/Assurance Program*
- [12] U.S. CIO Council, *Proposed Security Assessment & Authorization for U.S. Government Cloud Computing*
- [13] Microsoft, *Information Security Management System for Microsoft Cloud Infrastructure*
- [14] Microsoft, *Microsoft Compliance Framework for Online Services*
- [15] Microsoft, *Securing Microsoft's Cloud Infrastructure*
- [16] ISO/IEC16680 *The Open Group Service Integration Maturity Model (OSIMM)*
- [17] ITU-T Recommendation X.805 (2003), Security architecture for systems providing end-to-end communications.
- [18] ISO/IEC 18028-1:2006, Information technology - Security techniques - IT network security - Part 1: Network security management.
- [19] ISO/IEC 18028-2:2006, Information technology - Security techniques - IT network security - Part 2: Network security architecture.
- [20] ISO/IEC 18028-3:2005, Information technology - Security techniques - IT network security - Part 3: Securing communications between networks using security gateways.
- [21] ISO/IEC 18028-4:2005, Information technology - Security techniques - IT network security - Part 4: Securing remote access.
- [22] ISO/IEC 18028-5:2006, Information technology - Security techniques - IT network security - Part 5: Securing communications across networks using virtual private networks

- [23] ISO/IEC 18043:2006, Information technology - Security techniques - Selection, deployment and operations of intrusion detection systems.
- [24] ISO/IEC TR 18044, Information technology - Security techniques - Information security incident management.