ISO/IEC JTC 1/SC 27 N12429

ISO/IEC JTC 1/SC 27/WG 1 N112429

REPLACES: N11916

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC. TYPE: Working Draft text

TITLE: **Text for ISO/IEC 5th WD 27017 based on DoC (N12767) – 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, D. Turner, K. Nakao)

DATE: 2013-06-14

PROJECT: 1.27.91 (27017)

STATUS: **In accordance with Resolution 5 (contained in SC 27 N12440) of the 46th SC 27/WG 1 meeting in Sophia Antipolis (France) 26th April 2013, this document is circulated for STUDY AND COMMENT.**

Comments are to be returned to the SC27 Secretariat by 13th September 2013. PLEASE submit your comments / contributions on the herby attached document via the SC 27 e-balloting/commenting website at: http://isotc.iso.org/livelink/livelink/open/jtc1sc27

ACTION ID: **Study and Comment**

DUE DATE: 2013-09-13

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 + 66

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

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

Editors' notes

The revised text (SC27 N12429: WD5) is based on the discussions and resolutions from 27017 editing session in Sofie Antipolis. These notes summarize how the revised text (SC27 N12429: WD5) was produced based on DoC (SC27 N12767).

I. Important information on creation of the revised text (SC27 N12429: WD5)

1. SC27/WG1 Resolution 1

i. The following experts Mike Edwards, Laura Kuiper and Shin Yamashita, assisted the 27017 Editors in the preparation of the 5th WD text.

ii. This group of three experts is described as the "Editing Team".

iii. "Editing Team" provided recommendations to the editors as part of the preparation activity.

2. Steps for revising the text based on ISO/IEC 27017 DoC (SC27 N12767)

i. All resolutions of the editing session in Sophia Antipolis have been incorporated into the revised text.

ii. The recommendations of the Editing Team based on SC27 WG1 Resolution 1 have been incorporated into the revised text.

iii. The revised text has been adjusted based on the structure of ISO/IEC 27002 FDIS.

II. Information for NBs and liaisons to create comments and contributions

1. Circulated documents

i. SC27 N12767: DoC (Revised N12428)

ii. SC27 N12429: Revised text (WD5)

2. Considerations for creating comments and contributions

i. To create comments and considerations on the revised text (SC27 N12429:WD5)

ii. To refer DoC (SC27 N12767) including an explanation on how the revised text (SC27 N12429:WD5) has been developed based on all resolutions of Sophia Antipolis and the recommendations of the Editing Team.

Contents

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 for cloud service providers and cloud service customers 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.

0.2 Needs

One of the primary concerns with the use of cloud services is how cloud service customer(s) can obtain services from cloud service provider(s), in a manner that meets the cloud service customer's information security requirements. There is a need to provide cloud service customers with information to help them choose cloud services and a means by which they should evaluate the information security aspects of those cloud services.

0.3 Objectives

The objectives of this International Standard are to provide a security control framework and implementation guidance for both cloud service customers and cloud service providers.

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

Adoption of cloud service is expected to reduce IT capital and operating costs. However, there are additional security considerations to consider along with the anticipated benefits.

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

1 Scope

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

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

This International Standard provides implementation guidance for both providers and consumers of cloud services.

2 Normative references

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

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

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

3 Definitions and abbreviations

3.1 Terms and definitions

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

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

[ISO/IEC 2nd CD 17788]

3.1.2 capability
quality of being able to perform a given activity
[ISO 19440:2007]

3.1.3 cloud capability type

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

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

[ISO/IEC 2nd CD 17788]

3.1.4 cloud computing

paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with on-demand self-service provisioning and administration

NOTE – Examples or resources include servers, operating systems, networking, software, and storage equipment.

[ISO/IEC 2nd CD 17788]

3.1.5 cloud service

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

[ISO/IEC 2nd CD 17788]

3.1.6 cloud service category

group of **cloud services** (3.1.5) that possess some qualities in common with each other

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

[ISO/IEC 2nd CD 17788]

3.1.7 cloud service customer

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

[ISO/IEC 2nd CD 17788]

3.1.8 cloud service provider

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

[ISO/IEC 2nd CD 17788]

3.1.9 cloud service user

person associated with a **cloud service customer** (3.1.7) that uses **cloud services** (3.1.5)

[ISO/IEC 2nd CD 17788]

3.1.10 IaaS (Infrastructure as a Service)

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

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

[ISO/IEC 2nd CD 17788]

3.1.11 Infrastructure capabilities type

cloud capabilities type (3.1.3) in which the **cloud service customer** (3.1.7) can provision and use processing, storage and networking resources so that they are able to deploy and run

arbitrary software
[ISO/IEC 2nd CD 17788]

3.1.12 PaaS (Platform as a Service)

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

[ISO/IEC 2nd CD 17788]

3.1.13 party
natural person or organization
[ISO/IEC 2nd CD 17788]

3.1.14 platform capabilities type
cloud capabilities type (3.1.3) in which the **cloud service customer** (3.1.7) can deploy, manage and run customer-created or customer-acquired applications using programming language specific execution environment supported by the **cloud service provider** (3.1.8)
[ISO/IEC 2nd CD 17788]

3.1.15 SaaS (Software as a Service)

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

[ISO/IEC 2nd CD 17788]

3.1.16 tenant
group of **cloud service users** (3.1.9) sharing access to a set of physical and virtual resources
NOTE – Typically, and within the context of multi-tenancy, the group of **cloud service users** (3.1.9) that form a tenant will all belong to the same **cloud service customer** (3.1.7) organization. There might be cases where the group of **cloud service users** (3.1.9) involves users from multiple different customers, particularly in the case of community cloud deployments, but these are specialized exceptions. However, a given **cloud service customer** (3.1.7) organization might have many different tenancies with a single **cloud service provider** (3.1.8), perhaps representing different business groups within the organization (e.g. sales versus accounting), since there may be good reason to keep the data and activities belonging to those different groups well separated for business and commercial reasons.
[ISO/IEC 2nd CD 17788]

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

ASN: Autonomous System Number
CPU: Central Processing Unit
EDoS: Economic Denial of Sustainability
IaaS: Infrastructure as a Service
ISP: Internet Service Provider
PaaS: Platform as a Service
SaaS: Software as a Service
SIEM: Security Information and Event Management
SSL: Secure Sockets Layer
TLS: Transport Layer Security
VLAN: Virtual Local Area Network

4 Overview

4.1 Structure of this standard

This International Standard is 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.

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

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

- Information Security Policies (Clause 5)
- Organization of information security (Clause 6)
- Human Resource Security (Clause 7)
- Asset management (Clause 8)
- Access Control (Clause 9)
- 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 one or more of the 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 x.x.x and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

Sector-specific guidance for cloud services

provides the description “The following sector-specific guidance also applies.” followed by one of three types of description of the guidance of cloud services:
Type 1 covers the case where there is separate guidance for cloud service customer and for cloud service provider.
Type 2 covers the case where there is only guidance either for cloud service customer or for cloud service provider but not for both.
Type 3 covers the case where there is the same guidance for both cloud service customer and for cloud service provider.

Type 1

Cloud service customer	**Cloud service provider**

Type 2

Cloud service customer

or

Cloud service provider

Type 3

Cloud service customer	**Cloud service provider**

Other information for cloud computing

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

4.2 Relations with the other standards

This International Standard contains an overview, terms and definitions, control objectives, controls, implementation guidance and other information descriptions. This can be applied to an organization’s information security management in conformance with other ISMS family of standards as a sector/service-specific standard.

4.3 Relationships between cloud service customer and cloud service provider

4.3.1 Relationship between cloud service customer and cloud service provider

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

4.3.2 Supplier relationships in cloud computing services

The following supplier relationships should be considered in cloud computing:

a) the relationship of the cloud service provider to the cloud service customer, where the provider is the supplier

b) the relationship of a cloud service provider to a peer cloud service provider when the provider uses cloud services of the peer provider - in this case, the peer provider is the supplier

c) the relationship of a cloud service provider to a cloud service developer, where the developer is the supplier

4.4 Assessing information security risks in cloud services

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

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

Cloud service customer should consider the following when assessing information security risks for use of cloud services. It should be noted that the factors listed below might affect types of risk that are beyond the scope of this standard, as well as information security risk.

a) Information regarding information security controls disclosed by cloud service provider can be limited or abstracted in order to minimize risks to the cloud service provider associated with the disclosures. Cloud service providers can offer to provide more detailed information to a current or prospective cloud service customer using a NDA or other legal document to protect any disclosed information.

b) Disclosure of cloud service provider security information, risks and vulnerabilities, can expose all cloud service customers to risk due to the shared nature of the services.

c) Failure to disclose a known vulnerability or exploit relating to a cloud service, or the cloud resources used by the service, poses a risk to the cloud service customer.

d) A contractual risk can arise from a cloud service agreement, particularly where the cloud service provider operates in a different jurisdiction from that of the cloud service customer.

e) The cloud service customer should take into account the legal risks that may not protect his rights in cloud service provider jurisdiction

f) Risk can arise when cloud service customers and cloud service providers are in different jurisdictions.

g) The cloud service customer should consider additional threats and vulnerabilities when assessing information security risks when using cloud services. It should be noted that the

factors listed in Annex D might affect types of risks that are beyond the scope of this standard.

h) IT and telecommunication availability risks associated with the country where a cloud service provider is based, including the risk of natural disasters, telecommunication disruption and specific physical or cyber-attacks in such country or geopolitical region.

i) The use of cloud services implicates dependence on the cloud service provider. When the cloud service customer retires a cloud service, or when the cloud service provider goes out of business, data availability and portability of the respective cloud service needs to be considered in advance.

5 Information 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 service customer
Cloud service customer should consider different information security threats between on-premise and cloud computing environments. An information security policy for the use of cloud computing should be commensurate with the organization's acceptable levels of information security risks for their information and other assets. When defining the information security policy for the use of cloud computing, cloud service customer should take the following into account: a) information stored in the cloud computing environment that is subject to access and management by the cloud service provider; b) assets maintained in the cloud computing environment, e.g. application programs; c) processes run on the cloud service; d) individual users of the cloud service; e) administrators appointed within the cloud service customer who have privileges. When selecting a cloud computing service, cloud service customer should negotiate with cloud service provider on information security levels and service specifications to ensure compliance with the cloud service customer's policy. Information security levels and service specifications are often defined by the cloud service provider and are non-negotiable. Cloud service customer should develop additional measures, including limiting the use of cloud computing, to adjust the given risk to its own acceptable level.

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 Organization of information security

6.1 Internal organization

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

6.1.1 Information security roles and responsibilities

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

Cloud service customer	**Cloud service provider**
The division of information security responsibilities between cloud service customer and cloud service provider should be clearly defined and documented.	

Cloud service customer
Different cloud service categories used by a cloud service customer will have different divisions of responsibilities between cloud service customer and cloud service provider. Therefore, for each type of cloud service used by a cloud service customer, the division of responsibilities should be defined and documented to ensure appropriate controls are identified and implemented. Management should approve assignment of specific roles and responsibilities for information security across the organization relevant to the use of cloud service.

6.1.2 Segregation of duties

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

6.1.3 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 service customer	**Cloud service provider**
Cloud service customer should identify the applicable supervisory authorities and jurisdiction. Cloud Computing can allow for information to be stored in a variety of locations. When using a cloud service, the cloud service customer should identify the location where that data and information are stored, in order to identify the applicable supervisory authorities and jurisdictions applicable for the location of the information.	Cloud service provider should maintain and provide the contact information for applicable cloud service supervisory authorities and make it available to the cloud service customer.

6.1.4 Contact with special interest groups

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

6.1.5 Information security in project management

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

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.

6.2.2 Teleworking

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

7 Human resource security

7.1 Prior to employment

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

7.1.1 Screening

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

7.1.2 Terms and conditions of employment

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

7.2 During employment

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

7.2.1 Management responsibilities

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

7.2.2 Information security awareness, education and training

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

Cloud service customer	Cloud service provider
Cloud service customer should add the following items to awareness, education and training programmes for cloud service users, including relevant employees, contractors and third party users if applicable: 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) System and network environment risks with the use of cloud service. Cloud service customer should request cloud service provider to offer user manuals, precautions and contacts regarding the cloud service for use in information security education,	Where applicable, the cloud service provider should issue user manuals, and contacts regarding the cloud service for the purpose of IS education, training and awareness programme of cloud service.

training, and awareness programmes. Information security education, training and awareness about cloud services should be provided to management and the supervising managers, including those of business units, as part of information security co-ordination for effective co-ordination of information security activities. Cloud service customer should provide opportunities to share and exchange information about use of cloud service.	

7.2.3 Disciplinary process

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

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.

8 Asset management

8.1 Responsibility for assets

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

8.1.1 Inventory of assets

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

Cloud service customer	**Cloud service provider**
Asset management by cloud service customer should be valid for cloud service customer's assets maintained in the cloud computing environment. Cloud service customer should confirm that the cloud service provides functions supporting asset management by the cloud service customer.	Cloud service provider should provide cloud service functions that support asset management of cloud service customer's assets maintained in the cloud service environment.

Other information for cloud computing

Cloud service customer's assets maintained in the cloud service environment can include the followings:

a) business information;
b) virtualized equipment;
c) virtualized storage;
d) software.

Kinds of cloud service customer's assets vary depending upon the cloud services. Software used for provision of SaaS can be cloud service customer's asset for the SaaS provider in relation with IaaS as its infrastructure.

8.1.2 Ownership of assets

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

8.1.3 Acceptable use of assets

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

8.1.4 Return of assets

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

Cloud service customer
Cloud service customers should ensure that arrangements are made for the return of assets in a timely manner, upon termination of employment, contract or agreement with the cloud service provider. .

8.2 Information classification

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

8.2.1 Classification of information

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

8.2.2 Labelling of information

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

8.2.3 Handling of assets

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

8.3 Media handling

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

8.3.1 Management of removable media

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

8.3.2 Disposal of media

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

8.3.3 Physical media transfer

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

9 Access control

9.1 Business requirements of access control

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

9.1.1 Access control policy

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

9.1.2 Access to networks and network services

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

Cloud service customer	Cloud service provider
Cloud service customer should include the following regarding control on the use of cloud service in the policy on the use of network services: a) access control for each cloud service customer to the services provided by cloud service provider; b) access controls preventing network access from designated sites or environments to the cloud service. Cloud service customer should request the specification on types of information relevant to controlling use of cloud service for the purpose of developing policy on the use of network services.	The cloud service provider should provide specifications on the network access control features relating to the use of cloud services by cloud service customers, including: a) user credentials required for the cloud service customers to access cloud services; b) endpoint address details for the cloud service, such as the URL or IP address and port number.

9.2 User access management

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

9.2.1 User registration and de-registration

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

9.2.2 User access provisioning

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

9.2.3 Management of privileged access rights

Control 9.2.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

9.2.4 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 service customer	Cloud service provider
Where password management tools and processes are part of the cloud service, the cloud service customer should confirm that formal management process for allocation of password is realized by the functionality provided by the cloud service provider.	Cloud service provider should provide the following information on password allocation to the cloud service customer to enable allocation of passwords through a formal management process: a) procedures of issuance, change and re-issuance of password; b) authentication and authorization methods in allocation of passwords including applied multi-factor authentication techniques.

9.2.5 Review of user access rights

Control 9.2.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

9.2.6 Removal or adjustment of access rights

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

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 service customer	Cloud service provider
Cloud service customer should restrict access to cloud services, cloud service functions and cloud service customer's information maintained in the service by its cloud service users and by customer cloud service administrators in accordance with the organization's access control policy. (see 13.1.1) Cloud service customer should request to the cloud service provider with specifications of access restrictions to the cloud service, cloud service functions and cloud service customer's information.	Cloud service provider should provide the following information to the cloud service customer for access restriction on the cloud service customer's information: a) functional specifications of access restriction that are made available to the cloud service customer to the cloud service, cloud service functions and cloud service customer's information maintained in the service; b) specifications of access restriction that restrict access by the cloud service provider to the cloud service customer's information.

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.

9.4.3 Password management system

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

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 service customer	Cloud service provider
Cloud service customer should restrict and should tightly control the use of utility programs running in the cloud environment that might be capable of overriding system and application controls. Cloud service customer should request the following information to the cloud service provider to restrict and control the use of utility programs accessing cloud service: a) specifications of utility programs that might be capable of overriding system and application controls; b) functional specifications to restrict and control utility programs.	Cloud service provider should restrict and should tightly control the use of utility programs that might be capable of overriding system and application controls.

Other information for cloud computing

System administrator oriented capabilities of the cloud service can be provided as utility programs that might be capable of overriding system and application controls. Use of these programs by end users of a cloud service customer should be restricted and tightly controlled.

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 service customer
Cloud service customer should confirm that functionalities of cryptography provided on cloud service are adequate with the policy on the use of cryptographic controls on cloud service. Cloud service customer should request information to the cloud service provider to confirm that encryption functionalities provided on cloud service are adequate with the cryptographic policy on the use of cryptographic controls.

10.1.2 Key management

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

Cloud service customer	**Cloud service provider**
Cloud service customer should identify cryptographic keys to be managed by the cloud service customer on cloud service, and establish the procedure of key management. Cloud service customer should request the following information on procedures used to manage keys related to cloud service: 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, storing, retiring, retrieving, retaining and destroying; c) recommended key management procedures for use by customer." The Cloud service customer should not permit the cloud service provider to store and manage encryption keys on behalf of the cloud service customer for protection of any data that is owned or managed by the cloud service customer; rather, the cloud service	Cloud service provider should provide the following information on key management service to support the cloud service customer in use of the service: 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, storing, retiring, retrieving, retaining and destroying; c) recommended key management procedures for use by cloud service customer. The cloud service provider should provide capabilities to permit the cloud service customer to independently store and manage encryption keys used for protection of any data owned or managed by the cloud service customer.

customer should employ a separate and distinct service to store and manage keys.	

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 service customer	Cloud service provider
Cloud service customer should request information about physical security perimeter to confirm that the specification satisfies the cloud service customer's requirements.	If appropriate, cloud service provider should provide specifications of physical security perimeter to support the cloud service customer in confirming the specifications against its requirements.

Other information for cloud computing

Cloud service provider should consider the trade-off between support of the cloud service customers and information security risks when it decides the scope of information on physical security perimeters and associated controls to be provided to the cloud service customers.

11.1.2 Physical entry controls

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

11.1.3 Securing offices, rooms and facilities

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

11.1.4 Protecting against external and environmental threats

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

11.1.5 Working in secure areas

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

11.1.6 Delivery and loading areas

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

11.2 Equipment

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

11.2.1 Equipment siting and protection

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

11.2.2 Supporting utilities

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

11.2.3 Cabling security

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

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.

12.1.2 Change management

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

Cloud service customer	Cloud service provider
Cloud service customer should manage changes by cloud service provider on systems and services that affect information security of cloud service customer's organization within cloud service customer's change management process.	Cloud service provider should provide the following information regarding changes to the systems and services that affect information security of cloud service customer's organization for cloud service customer to manage changes: a) planned date and time of system changes; b) changes to the system; c) announcement of system change start and completion;

Other information for cloud computing

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

Security attestations are useful, related to systems and services that represent shared infrastructure with other cloud service customers from the cloud service provider.

12.1.3 Capacity management

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

Cloud service customer	Cloud service provider

Cloud service customer should confirm that the capacity that it has agreed to obtain from the cloud service is sufficient to deliver the cloud service customer's required system performance. Cloud service customer should monitor its usage of cloud service resources and reconfigure those resources so that the cloud service customer's requirements for system performance are met. Cloud service customer should project its future system performance requirements and use 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 service provider. Cloud service customer should confirm that a cloud service provider can deliver the capacity and required and future system performance for a cloud service.	Cloud service provider should provide the following information to the cloud service customer to enable its capacity management: a) system environment: 1) capacity of 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) lead time to have additional capacity or system performance, and minimum unit of the addition; 4) maximum capacity and system performance; b) statistics on system resource usage: 1) statistics in a given time period; 2) maximum system resource usage. c) Limitations on additional resource provisioning to cloud service customer; d) Statistical information on resource provisioning failures either relating to specific cloud service customer account or service-wide, as well as average resource provisioning times. Cloud service provider should monitor total volume of logical computing resource of cloud computing environment considering total volume of physical capacity to prevent severe information security incident.

Other information for cloud computing

Cloud service customer can consider the followings in capacity management if such information is provided by the cloud service provider;

a) system environment;
   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

b) statistics on system resource usage
   1) statistics in a given time period
   2) maximum system resource usage

Total volume of logical capacity can never exceed the total volume of physical capacity. If volume of resource requirement exceeded total volume of physical capacity, it may cause severe incident. For the reason, monitoring the total volume of logical computing resource and keep certain volume of available resource is required to prevent incidents caused by lack of resource.

12.1.4 Separation of development, testing and operational environments

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

12.2 Protection from malware

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

12.2.1 Controls against malware

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

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 service customer	Cloud service provider
Cloud service customer should define back-up policy, and develop procedures considering the followings: a) back-up and restoration functions should be performed as part of the cloud service; b) back-up and restoration functions that need be developed by the cloud service customer; c) backups should be encrypted according to the policy on the use of cryptographic controls (see ISO/IEC 27002, 10.1.1); d) local and or off-site storage of back-ups should be documented; e) retention period for back-up data.	Cloud service provider should provide the specifications of back-up function to the cloud service customer to support developing cloud service customer's back-up policy and procedures. The specifications can include the followings as appropriate to the cloud service: a) scope and schedule of back-ups; b) back-up methods and data formats; c) frequency of backups; d) version control for back-up data; e) governing jurisdictions of customer data back up; f) procedure to verify integrity of back-up data; g) procedure to restore from back-up.

	h) procedure to test functionality of complete back-up routines; i) service specifications such as a real-time portal or console view of the backup systems

12.4 Logging and monitoring

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

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 service customer	Cloud service provider
Cloud service customer should request specifications to the cloud service providers to develop procedures for monitoring usage of the cloud computing services, e.g.: a) type of usage records; b) retention period of usage records.	Cloud service provider should provide the following specifications to the cloud service customer to develop procedures for monitoring usage of the cloud computing services: a) type of usage records; b) retention period of usage records.

12.4.2 Protection of log information

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

12.4.3 Administrator and operator logs

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

12.4.4 Clock synchronisation

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

12.5 Control of operational software

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

12.5.1 Installation of software on operational systems

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

Cloud service provider
Where the cloud service provider has a service which enables a cloud service customer to upload software package(s) to the service and subsequently run that software, the cloud service provider's service environment should: a) keep track of each uploaded software package, including any modifications that may be done by the cloud service customer b) log when a particular software package is run c) monitor the running software, with a particular concern for any activities that appear to be malicious or likely to cause harm to the cloud service provider's system

12.6 Technical vulnerability management

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

12.6.1 Management of technical vulnerabilities

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

Cloud service customer	Cloud service provider
Cloud service customer should understand technical vulnerability management of cloud service. In case the management is not compliant with cloud service customer' requirements, cloud service customers' own response should be considered. Cloud service customer should request the following information to the cloud service provider to understand technical vulnerability management. a) way to identify technical vulnerability; b) policy to respond technical vulnerability; d) request and agree upon criteria for system feature to be considered vulnerable	Cloud service 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. 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. Cloud service provider should not provide the cloud service customer of other cloud service customers' vulnerabilities.

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.

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.

Other information for cloud computing

Real-time portal or console for cloud service customer is useful tool for sharing information of the situation of cloud computing environment.

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 service customer
Cloud service customer should request service specifications related to networks including network capacity and redundancy to the cloud service providers in selecting a cloud computing service.

13.1.3 Segregation in networks

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

Cloud service customer	Cloud service provider
Cloud service customer should request information on functional specifications on dividing the networks into separate network domains, to the cloud service provider to segregate networks of cloud service.	The cloud service provider should enforce logical segregation of networking between cloud service customers, 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.

Other information for cloud computing

Examples of cases when requesting cloud service 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

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

14 System acquisition, development and maintenance

14.1 Security requirements of information systems

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

14.1.1 Security requirements analysis and specification

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

Cloud service customer	Cloud service provider
Cloud service customer should specify the security requirements for the cloud service. Cloud service customer should analyse and evaluate the alignment of the implemented controls in cloud service to the requirement. Cloud service customer should include cloud specific risks along with the organization's general information security risks as input to its information security risk assessment process and evaluate the differences of the risks between on-premise and cloud computing services. Use of cloud service can increase or sometimes decrease information security risks. Cloud service customer should be aware that visibility of controls and achieved levels of information security tends to be limited in the use of cloud service, and information security risks can be difficult to be identified.	Cloud service provider should provide information related to the implemented controls of cloud service to the cloud service customer to support analysing the alignment of control treatment between cloud service customer's requirement and the implemented controls in cloud service. The cloud service provider should implement suitable controls to ensure the isolation of different tenancies. Cloud specific risks for cloud service customer are also those for cloud service provider, which can be stated as the cloud service provider's business risks. Cloud service provider should provide information on the information security risks of cloud service to the cloud service customer. The information should be provided in appropriate level of description, e.g. as service level statement, risks with controls, or, in the case technical detail is required, control mechanisms, that suites the nature of the cloud service. Information security risks of a SaaS can be conveyed by service level description, while provider of SaaS running on IaaS can require descriptions that include control mechanisms of the infrastructure.

14.1.2 Securing applications services on public networks

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

14.1.3 Protecting application services transactions

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

14.2 Security in development and support processes

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

14.2.1 Secure development policy

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

14.2.2 System change control procedures

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

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.

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 Secure system engineering principles

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.

Other information for cloud computing

In the case of cloud computing, the idea of system acceptance testing mainly applies to the cloud service itself and the use of the cloud service by the cloud service customer. In this clause, it is the use of the cloud service by the cloud service customer that is subject to guidance.

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

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 service provider
Where a cloud service provider uses cloud services of a peer cloud service provider, the service agreement between the provider and the peer provider should contain security obligations on the peer provider that at least match the security requirements placed on the provider by the agreement(s) which the provider has with their cloud service customers.

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 service provider
Cloud service provider should provide service specifications including information security controls that will be addressed in agreements to support candidate cloud service customer in evaluating the controls against its information security policy on supplier relationship or use of cloud computing. Service Delivery of the cloud service provider should match the policy requirements of the cloud service customer and the legal requirements of the contract between the cloud service provider and the cloud service customer. When cloud service provider provide cloud computing service based on supply chain, cloud service provider should provide risk management objective to suppliers and request each of the suppliers to perform risk management activities to achieve the objective.

Other information for cloud computing

Some cloud service customers may place specific conditions into the cloud service agreement relating to the human resources of the cloud service provider involved in the delivery of the service. If the cloud service provider agrees to these conditions, then the cloud service provider is obliged to reflect these conditions with respect to their human resources and assignment to the project.

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 service provider
In case of cloud service provider that is a cloud service customer of other services, cloud

service provider should pass through the service levels of its suppliers. Cloud service provider should ensure that the service levels guaranteed to its cloud service customers do not interfere with lower service levels of its own suppliers.

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.

15.2.2 Managing changes to supplier services

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

16 Information security incident management

16.1 Management of information security incidents and improvements

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

16.1.1 Responsibilities and procedures

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

Cloud service customer
Cloud service customer should verify distribution process of information about severe information security incident by cloud service provider and be able to acquire information accurately. Cloud service customer should notice cloud service provider and have information to avoid affection of incident, when cloud service customer confirmed that incident occurred in the cloud computing environment.

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.

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.

16.1.4 Assessment of and decision on information security events

Control 16.1.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud Service Customer	**Cloud Service Provider**
Cloud service customer should verify the definition of information regarding severe information security incident provided by cloud service provider and information provision policy of cloud service provider, and review incident management framework upon needed.	Cloud service provider should define severe information security incident in the cloud environment, and define and document information provision policy regarding the incident, and notice to cloud service customer. Cloud service provider should define information of severe information security incident shared

	among supply chain, and document it after reaching agreement with suppliers.

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.

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 service customer	**Cloud service provider**
Cloud service customer should a) identify information that can serve as evidence that resides within a cloud service or within the cloud service provider environment associated with the cloud service b) establish procedures by which the information can be collected and acquired from the cloud service or the related provider environment c) ensure that information which can serve as evidence is preserved within the cloud service and related provider environment Ideally, the handling of this information should be covered by the cloud service agreement. Cloud service customer should request information to cloud service provider, when cloud service provider manages the information that might be legal evidence for cloud service customer:	The cloud service provider should give consideration to information held within a cloud service or within the cloud service provider environment associated with a cloud service, which can serve as evidence. When agreed, the cloud service provider should: a) document the information that can serve as evidence (and provide such documentation to customers) b) establish procedures for retaining such information, including retention period c) establish procedures by which a customer can request and obtain access to such information. Where there are costs and charges associated with such access, they should be documented to the customer d) in multi-tenant environments, ensure isolation of the information relating to different tenants and ensure that a particular customer only has access to the information that relates to that customer. e) ensure compliance of information recording and retention with the requirements of the jurisdiction that applies to the cloud service. Note: this can involve the jurisdiction that applies to the cloud service customer as well as that which applies to the cloud service provider. f) Description of the process for forensic support, if available;

	g) available information (from VMs, network, SIEM, offline VMs, IPS and other sources) h) Interfaces and APIs forensic information will be provided through, if available; i) protection measures against collateral damage during a forensic investigation on shared resources if available; j) protection of sensitive information from other tenants during a forensic investigation on shared resources like RAM or Network if available; k) Competence of available personnel supporting forensic investigations, l) provider awareness of local laws m) Procedures and measures to strictly isolate customer related evidence data if available. Cloud service provider should consider data protection constraints and best practices in dealing on data retention.

1
2

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.

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.

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.

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.

18 Compliance

18.1 Compliance with legal and contractual requirements

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

18.1.1 Identification of applicable legislation and contractual requirements

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

Cloud service customer	Cloud service provider
Cloud service customer should identify domestic and foreign legal, regulatory and contractual requirements depending on purpose of cloud service use.	Cloud service provider should provide information on legal and regulatory requirements of the country or region from where the cloud service is provided. Where cloud service provider uses upstream cloud services, their jurisdictions and applicable laws and regulations should be identified documented and kept up to date by the cloud service provider. When agreed cloud service provider should monitor for compliance to ensure customer data is contained within applicable geo-location or legislative jurisdictional restrictions. When cloud service provider provides cloud computing service based on various countries/regions with their own law enforcement, cloud service provider should make cloud service customer know about the countries/regions. Cloud service provider should verify that laws and regulations are different depending on federation of nations, countries, states, and towns, and show each of their name clearly enough to cloud service customer recognize each of them. Cloud service provider should show clearly the place of each jurisdiction of tribunals for each of the laws and regulations.

18.1.2 Intellectual property rights (IPR)

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

18.1.3 Protection of records

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

18.1.4 Privacy and protection of personally identifiable information

Control 18.1.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
Cloud service customer 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 service customer should request information on domestic and foreign legal and regulatory requirements of data protection and privacy of personal information to the cloud service provider to clarify legal and regulatory requirements of the country or region from where cloud service is provided.	Cloud service provider should provide information on legal jurisdiction that affects cloud service to the cloud service customer to support it identifying relevant legislation to data protection and privacy of personal information. Cloud service 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 service customer.

Other information for cloud computing
ISO/IEC 27018 Code of practice for data protection controls for public computing services can be referred to this subject.

18.1.5 Regulation of cryptographic controls

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

Cloud service customer
Cloud service customer should request cloud service provider to affirm that cryptographic technology used is not in conflict with regulations on export in the countries or regions where such cryptography is provided.

18.2 Information security reviews

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

18.2.1 Independent review of information security

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

18.2.2 Compliance with security policies and standards

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

Cloud service provider
Cloud service providers need to ensure that there are procedures in place to ensure compliance with security terms contained in the service agreements (and SLAs) with their cloud service customers.

18.2.3 Technical compliance review

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 service customer	**Cloud service provider**
Cloud service customer should confirm information related to technical compliance checking provided from the cloud service provider. When it does not satisfy cloud service customer technical compliance policy, cloud service customer should reconsider the use of the cloud service.	Cloud service provider should provide the policy of information provision about technical compliance checking, such as: a) objects; b) methods; c) frequency; d) results; e) corrective action for non-compliances Cloud service provider should provide cloud service customer the information about compliance checking according to the policy.

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

This Annex provides additional objectives and controls with 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.

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

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

CLD.6.3.1 Demarcation of responsibility

Control

Demarcation of responsibility between organizations of cloud service customer and providers should be defined and documented.

Implementation guidance

Cloud service customer	Cloud service provider
Cloud service customer should identify and manage the support contact and the customer contact of the cloud service provider. Cloud service customer should request information to the cloud service provider to maintain the contacts updated. Cloud service customer should review proposed demarcation of information security responsibilities and confirm if it can accept its responsibilities. Responsibilities of both parties should be stated in the agreement.	Cloud service provider should define and document demarcation of responsibilities of cloud service customer, cloud service provider and supplier. When agreed, cloud service provider should define and document sub-contractor responsibilities.

Other information for cloud computing

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

CLD.6.3.2 Information sharing system

Control

Information sharing system between cloud service customer and cloud service provider should be developed and maintained.

Implementation guidance

Cloud service customer	Cloud service provider
Cloud service customer should identify and manage the support contact and the customer contact of the cloud service provider.	Cloud service provider should define and present the information of what affect to information security.

Cloud service customer should request information to the cloud service provider to maintain the contacts updated.	Cloud service provider should identify and manage the customer contact of the cloud service customer. .

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

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

CLD.9.5.1 Protection of virtual environment

Control

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

Implementation guidance

Cloud service provider
Cloud service provider should control cloud computing resources assigned to a cloud service customer inaccessible by other cloud service customers and unauthorized users, to ensure segregation of virtual environments. This segregation should be strictly preserved regardless of physical configurations or physical migration of virtual assets.

Other information for cloud computing

In the case that virtual environment is provided by software virtualization function, e.g. virtual operating system, network and storage configurations can be virtualized, and segregation of physical networks can be made invalid. Segregation from other cloud service customers on software virtualized environment should be designed and implemented using segregation function of the software.

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

CLD.12 Operations security

CLD.12.4 Logging and monitoring

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

CLD.12.4.5 Operation log of cloud service customer privilege

Control

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

Implementation guidance

Cloud service provider
If privileged operation for cloud computing environment was delegated to cloud service customer, operation log by both of cloud service provider and cloud service customer should be acquired and stored to clarify boundary of responsibility.

CLD.13 Communications security

CLD.13.1 Network security management

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

CLD.13.1.4 Cooperation of configurations between virtual and physical network

Control

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

Implementation guidance

Cloud service provider
Cloud service provider should define and document policy requests of virtual network configuration cooperating to physical network security policy. Cloud service provider should prepare configuration manual based on virtualized security policy and provide it to operators.

Other information for cloud computing

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

CLD.16 Information security incident management

CLD.16.1 Management of information security incidents and improvements

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

CLD.16.1.8 Implementation of quick distribution process of information about information security incident on cloud computing environment

Control

Quick distribution process of information about information security incident on cloud computing environment should be implemented to share information with cloud service customer immediately after incident occurred.

Implementation guidance

A.1.1 Cloud service customer	**Cloud service provider**
Cloud service customer should verify distribution process of information about severe information security incident by cloud service provider and be able to acquire information accurately. Cloud service customer should notice cloud service provider and have information to avoid affection of incident, when cloud service customer confirmed that incident occurred in the cloud computing environment.	Cloud service provider should implement distribution process of information, to provide information about severe information security incident in the cloud computing environment to cloud service customer in appropriate time. For the information distribution process, various ways includes but not limited to real-time display on cloud service provider's web site, ad-hoc post, and periodic post. Cloud service provider should setup contact for severe incident. Cloud service provider should setup contact for

	information about severe incident which was detected by cloud service customer. If possible, cloud service provider should have agreement to share severe information security incident in supply chain, to share accurate information mutually.

1
2

Annex B: Information security risk related cloud computing

While security and privacy concerns when using cloud computing services are similar to those of traditional non-cloud services, concerns are amplified for the cloud service customer by external control over organizational assets and the potential for mismanagement of those assets. Transitioning to public cloud computing involves a transfer of responsibility and control to the cloud service provider over information as well as system components that were previously under the customer organization's direct control. The transition is usually accompanied by loss of direct control over the management of operations and also a loss of influence over decisions made about the computing environment.

Despite this inherent loss of control, the cloud service customer still needs to take responsibility for their use of cloud services in order to maintain situational awareness, weigh alternatives, set priorities, and effect changes in security and privacy that are in the best interest of the organization. The customer achieves this by ensuring that the contract with the provider and its associated service level agreement (SLA) has appropriate provisions for security and privacy. In particular, the SLA must help maintain legal protections for privacy relating to data stored on the provider's systems. The customer must also ensure appropriate integration of the cloud services with their own systems for managing security and privacy.

There are a number of security risks associated with cloud computing that must be adequately addressed, both for the cloud service customer and for the cloud service provider:

	Cloud service customer	**Cloud service provider**
Threats	• Loss of governance • Responsibility ambiguity • Isolation failure • Vendor lock-in • Compliance and legal risks • Handling of security incidents • Management interface vulnerability • Data protection • Malicious behaviour of insiders • Business failure of the provider • Service unavailability • Migration and integration failures • Evolutionary risks • Cross-border issues • Insecure or incomplete data deletion	• Responsibility ambiguity • Inconsistency and conflict of protection mechanisms • Isolation failure • Unauthorized access to the provider's systems. • Jurisdictional conflict • Insider Threats • Supply Chain vulnerability

A.1 Threats for cloud service customers

The following threats are those that directly affect the cloud service customers, in that they may affect the cloud service customers personal or business interests, privacy, lawfulness, or safety. Not all cloud service customers will be at risk from all threats, or the risk will be unequal depending on the nature of the cloud service customer and of the cloud service being used:

- **Loss of governance.** For public cloud deployments, customers necessarily cede control to the cloud provider over a number of issues that may affect security. At the same time, cloud service level agreements (SLA) may not offer a commitment to provide such capabilities on the part of the cloud service provider, thus leaving gaps in security defences.

- **Responsibility ambiguity**. Given that use of cloud computing services spans across the customer and the provider organizations, responsibility for aspects of security can be spread across both organizations, with the potential for vital parts of the defences to be left unguarded if there is a failure to allocate responsibility clearly. The split of responsibilities between customer and provider organizations is likely to vary depending on the model being used for cloud computing (e.g. IaaS versus SaaS).
  There is also a requirement for the service agreement, the SLAs and the cloud service description to be clear on the security and privacy facilities associated with the cloud service.

- **Isolation failure.** Shared resources and multi-tenancy are defining characteristics of public cloud computing. This risk category covers the failure of mechanisms separating the usage of data, storage, memory, routing and even reputation between different tenants (e.g., so-called guest-hopping attacks).

- **Vendor lock-in**. Dependency on proprietary services of a particular cloud service provider could lead to the cloud service customer being tied to that provider. Services that do not support portability of applications and data to other providers increase the risk of data and service unavailability.

- **Compliance and legal risks.** Investment in achieving certification (e.g., industry standard or regulatory requirements) may be put at risk by migration to use cloud computing if the cloud service provider cannot provide evidence of their own compliance with the relevant requirements or if the cloud provider does not permit audit by the cloud service customer. It is the responsibility of the customer to check that the provider has appropriate certifications in place, but it is also necessary for the cloud customer to be clear about the division of security responsibilities between the consumer and the provider and to ensure that the customer's responsibilities are handled appropriately when using cloud services.

- **Handling of security incidents**. The detection, reporting and subsequent management of security breaches is a concern for cloud service customers, who are relying on the provider to handle these matters.

- **Management interface vulnerability.** Customer management interfaces of a public cloud provider are usually accessible through the Internet and mediate access to larger sets of resources than is typical with traditional hosting providers and therefore pose an increased

risk, especially when combined with remote access and web browser vulnerabilities.

- **Data protection.** Cloud computing poses several data protection risks for cloud customers and providers. The major concerns are exposure or release of sensitive data but also include loss or unavailability of data. In some cases, it may be difficult for the cloud service customer (in the role of data controller) to effectively check the data handling practices of the cloud service provider and thus to be sure that the data is handled in a lawful way. This problem is exacerbated in cases of multiple transfers of data, e.g., between federated cloud services.

- **Malicious behaviour of insiders**. Damage caused by the malicious actions of insiders working within an organization can be substantial, given the access and authorizations they may have. This is compounded in the cloud computing environment since such activity might occur within either or both the customer organization and the provider organization.

- **Business failure of the provider**. Such failures could render data and applications essential to the consumer's business unavailable.

- **Service unavailability**. This could be caused by a host of factors, from equipment or software failures in the provider's data centre, through failures of the communications between the customer systems and the provider services.

- **Migration and integration failures**. Migrating to use cloud services may involve moving data and applications from the customer environment to the provider environment, with associated configuration changes (e.g., network addressing). Migration of a part of the customer's IT infrastructure to a cloud service provider may require substantial changes in the infrastructure design (e.g. network and security policies). The migrated applications and data also require integration with other customer systems and this may fail resulting in both functional and non-functional impacts.

- **Evolutionary risks.** A cloud service that has passed the security assessment of the customer during the acquisition phase might have new vulnerabilities introduced during its lifetime due to changes in software components introduced by the cloud service provider.

- **Cross-border issues**. One feature of cloud computing is that the cloud service provider's systems may be located in a different jurisdiction to that of the customer – or the provider's systems may be split across multiple jurisdictions. This is a problem for the customer, since it may not be clear which regulations and laws will apply to the cloud service and to the data and applications associated with the service and could result in the customer breaching the regulations of the "home" jurisdiction.

- **Insecure or incomplete data deletion.** Requests to delete cloud resources, for example, when a customer terminates the use of a cloud service with a provider, may not result in complete deletion of the customer's data from the provider's systems. Adequate or timely data deletion may also be impossible, either because extra copies of data are stored but are not available, or because the disk to be deleted also stores data from other customers. In the case of multi-tenancy and the reuse of hardware resources, this represents a higher risk to the customer than is the case with dedicated hardware.

While these risks primarily apply to cloud service customers, it is important to note that they can also apply to a cloud service provider, where the provider depends on the cloud service of a peer cloud service provider.

A.2 Threats for cloud service providers

This clause considers threats that directly affect the cloud service provider. Such threats might affect the ability of the provider to offer a cloud service, to do business, to retain customers, and to avoid legal or regulatory difficulties. Threats to a given cloud service provider will depend on their specific service offerings and environments.

- **Responsibility ambiguity.** Given that use of cloud computing services spans across the consumer and the provider organizations, responsibility for aspects of security can be spread across both organizations. Ambiguity relating to roles and in the definition of responsibilities related to issues such as data ownership, access control and infrastructure maintenance may give rise to business or legal disputes.

- **Inconsistency and conflict of protection mechanisms.** Due to the decentralized architecture of a cloud infrastructure, its protection mechanisms might be inconsistent among distributed security modules. For example, an access denied by one Identity and Access Management (IAM) module may be granted by another. This inconsistency might cause problems for authorized user, and might be exploited by an attacker, thereby compromising both confidentiality and integrity.

- **Isolation failure.** Cloud computing typically involves resource sharing between multiple customers. There exists the potential for a failure of the isolation mechanisms that keep the data and applications of different customers separate. This risk is a threat to the reputation of the provider and to the provider's business. Unintended exposure of customer assets could be the cause of litigation

- **Unauthorized access to the provider's systems.** Cloud computing inevitably implies providing access to parts of the provider's systems for customer users and customer administrators. The risk is that this access might also inadvertently provide access to parts of the provider's systems only intended for use by authorized provider staff.

- **Jurisdictional conflict**. A cloud service provider may operate data centres in multiple jurisdictions and may move data between datacentres. Depending on the hosting country, data will be governed by different applicable jurisdictions – and may also be different to the jurisdiction that applies to any particular cloud service customer. Some jurisdictions, such as the EU, require extensive protection of personally identifiable information, which should not be processed in countries that do not provide a sufficient level of guaranteed protection. Treating data incorrectly can result in legal penalties.

- **Insider Threats.** Where humans are involved, there is always a risk of individuals acting in a malicious or careless manner that puts the security of the service at risk. Cloud service provider employees leaving credentials unsecure, malicious actions by disgruntled employees or skilled criminals gaining a position on the provider's staff all pose a significant threat to any business.

Appropriate controls need to be in place to limit access to customer data and applications and to monitor for any suspicious activities.

- **Supply chain vulnerability.** The trustworthiness of a cloud service provider is dependent on a vulnerability risk analysis of its supply chain. This risk analysis involves identifying and gathering information about the cloud service provider's acquired components for computing, networking, and storage that are used to provide cloud services. Typical cloud service provider supply chain security activities include:
    - Background information about the participants in the cloud service provider supply chain.
    - Validation of hardware, software and services used by the cloud service provider.
    - Inspection of the cloud service provider hardware and software when it is received to ensure that it was not tampered with while in-transit.

Bibliography

[1] ISO/IEC 17788, *Information technology — Distributed application platforms and services — Cloud computing ─ Overview and Vocabulary*

[2] ISO/IEC 17789, *Information technology — Distributed Application Platforms and Services — Cloud Computing — Reference Architecture*

[3] NIST, SP800-144 *Guidelines on Security and Privacy in Public Cloud Computing*

[4] NIST, SP800-145 *The NIST Definition of Cloud Computing（Draft）*

[5] NIST, *Effectively and Securely Using the Cloud Computing Paradigm*

[6] ENISA, *Cloud Computing Benefits, risks and recommendations for information security*

[7] ENISA, *Cloud Computing Information Assurance Framework*

[8] Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1*

[9] Cloud Security Alliance, *Top Threats to Cloud Computing V1.0*

[10] Cloud Security Alliance, *Domain 12: Guidance for Identity & Access Management V2.1*

[11] Cloud Security Alliance, *CSA Cloud Controls Matrix V1.1*

[12] ISACA, *Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives*

[13] ISACA, *Cloud Computing Management Audit/Assurance Program*

[14] U.S. CIO Council, *Proposed Security Assessment & Authorization for U.S. Government Cloud Computing*

[15] ISO/IEC16680 *The Open Group Service Integration Maturity Model (OSIMM)*

[16] ITU-T Recommendation X.805 (2003), Security architecture for systems providing end-to-end communications.

[17] ISO/IEC 18028-1:2006, Information technology - Security techniques - IT network security - Part 1: Network security management.

[18] ISO/IEC 18028-2:2006, Information technology - Security techniques - IT network security - Part 2: Network security architecture.

[19] ISO/IEC 18028-3:2005, Information technology - Security techniques - IT network security - Part 3: Securing communications between networks using security gateways.

[20] ISO/IEC 18028-4:2005, Information technology - Security techniques - IT network security - Part 4: Securing remote access.

[21] ISO/IEC 18028-5:2006, Information technology - Security techniques - IT network security - Part 5: Securing communications across networks using virtual private networks

[22] ISO/IEC 18043:2006, Information technology - Security techniques - Selection, deployment and operations of intrusion detection systems.

[23] ISO/IEC TR 18044, Information technology - Security techniques - Information security incident management.