

<b>COMMITTEE DRAFT</b> <b>ISO/IEC 2<sup>nd</sup> CD 27017</b>		Reference number: <b>ISO/IEC JTC 1/SC 27 N13916</b>	
Date: <b>2014-06-05</b>		Supersedes document SC 27 N13160	
THIS DOCUMENT IS STILL UNDER STUDY AND SUBJECT TO CHANGE. IT SHOULD NOT BE USED FOR REFERENCE PURPOSES.			
ISO/IEC JTC 1/SC 27 Information technology - Security techniques Secretariat: Germany (DIN)		Circulated to P- and O-members, and to technical committees and organizations in liaison for comments by: <b>2014-09-06</b> Please submit your comments via the online balloting application by the due date indicated.	
<b>ISO/IEC 2<sup>nd</sup> CD 27017</b> <b>Title: Information technology -- Security techniques – Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002</b>			
Project: 1.27.91 (27017)			
<b>Explanatory Report</b>			
<b>Status</b>	<b>SC 27 Decision</b>	<b>Reference documents</b>	
		<b>Input</b>	<b>Output</b>
<i>For details regarding previous development stages please refer to the 2<sup>nd</sup> page of the explanatory report.</i>			
<b>ISO/IEC 27017</b> <b>5<sup>th</sup> WD</b>	46th WG 1 meeting, Oct. 2013, resolutions 1, 2, 5 (N12440); Del. of Auth. f. 1 <sup>st</sup> CD as per resolution 13 of 25 <sup>th</sup> SC 27 Plenary, April 2013 (N12739).	SoCom (N12294); ISACA com. (N12179) ITU-T SG17 liaison (N12275); Draft DoC (N12355).	Liaisons to: ISACA (N12515); ITU-T SG17 (N12507); DoC (N12767, replaces N12428); Text f. 5 <sup>th</sup> WD (N12429).
<b>ISO/IEC 27017</b> <b>1<sup>st</sup> CD</b>	47th WG 1 meeting, Oct. 2013, resolutions 1, 12, 26 (N13440)	SoCom (N12887); CA com. (N13068); ISACA com. (N12893); ITU-T SG17 liaison + com. (N12894); Draft DoC (N13107).	Request/endorsement limit dates extension (N13448 / N13nnnl); Liaison to: ITU-T SG 17 (N13174); DoC (N13159); Text f. 1 <sup>st</sup> CD (N13160).
<b>ISO/IEC 27017</b> <b>2<sup>nd</sup> CD</b>	48th WG 1 meeting, April 2014, Resolutions 1, 6, 9, 21, 23 (N13900); 26 <sup>th</sup> SC 27 Plenary, as per Resolution 8 Delegation of Authority for DIS (N14200).	SoV (N13563); CSA com. (N13638); ISACA com. (N13634); ITU-T SG17 liaison (N13563); Draft DoC (N13641).	Request/endorsement limit dates extension (N13448 / N13407); Request f. title change (N13927); Liaisons to: ISACA (N13949); TRESPASS (N13957); DoC (N13907); Text f. 2 <sup>nd</sup> CD (N13916).
<b>2<sup>nd</sup> CD Consideration</b> In accordance with resolution (see SC 27 N13900) of the 48 <sup>th</sup> SC 27/WG 1 Plenary meeting held in Hong Kong, China, 11 <sup>th</sup> April 2014 the hereby attached document is herewith circulated for a 2 <sup>nd</sup> Committee Draft (CD) letter ballot closing by  <b>2014-09-06</b>  <b>MEDIUM:</b> <a href="http://isotc.iso.org/livelink/livelink/open/jtc1sc27">http://isotc.iso.org/livelink/livelink/open/jtc1sc27</a>  <b>NO OF PAGES: 2 + 60</b>			

Explanatory Report (2 <sup>nd</sup> page)			
Status	SC 27 Decision	Reference documents	
		Input	Output
<b>Joint WG1/475 study period on cloud computing security and privacy</b>	41 <sup>st</sup> WG 1, 4, 5 meetings, Oct. 2010, resolutions (N9420, N9084, N9402)	GB rapporteur nomin. (N9442); JP contr. (N9044); JP present. (N9410); ISACA contr. (N9542); ISF contr. (N9408); ITU-T SG 17 liaison + contr. (N9470).	Call f. contr. (N9471).
<b>NWIP 1<sup>st</sup> WD</b>	42 <sup>nd</sup> WG 1 meeting, April 2011, resolutions 1, 4 (N10100); 22 <sup>nd</sup> SC 27 Plenary April 2011, resolution 20 (N10101)..	US contr. (N9850, N9851). ITU-T FG Cloud liaison (N10073).	SP reports(N10027, N10028); Future direction (N10036); Call f. contr. (N10035); NWIP (N10029).
<b>ISO/IEC NP 27017 2<sup>nd</sup> WD</b>	43 <sup>rd</sup> WG 1 meeting, Oct. 2011, resolutions 1, 4, 25 (N10570).	BE contr. (N10119); ITU-T SG 17 liaison + contr. (N10339). JTC 1/SC 7 li. + com. (N10201); SP report (N10220); SoV (N10212).	Liaisons to: ITU-T FG Cloud (N10600); DoC (N10593); Text f. 2 <sup>nd</sup> WD (N10594).
<b>ISO/IEC NP 27017 2<sup>nd</sup> WD</b>	43 <sup>rd</sup> WG 1 meeting, Oct. 2011, resolutions 1, 4, 25 (N10570).	BE contr. (N10119); JTC 1/SC 7 li. + com. (N10201); SoV (N10212).	Liaisons to: ITU-T FG Cloud (N10600); DoC (N10593); Text f. 2 <sup>nd</sup> WD (N10594).
<b>ISO/IEC 27017 3<sup>rd</sup> WD</b>	44 <sup>th</sup> WG 1 meeting, May 2012, resolutions 1, 6, 22, 26 (N11101). 24 <sup>th</sup> SC P (N11101).	SoCom (N10830); INLAC com. (N10963); ISACA (N10927); ITUT FG Cloud (N10678); AU (N10966); SG (N11065); SoC (N10830); Draft DoC (N11068).	Liaisons to: CSA (N11140); INLAC (N11132); ISF (N11141); ITU-T SG 13 (N11153); ITU-T SG 17 (N11135); ITU-T FG Cloud (N11139); Meet. rep (N11124); DoC (N11121); Text f. 3 <sup>rd</sup> WD (N11122).
<b>ISO/IEC 27017 4<sup>th</sup> WD</b>	45 <sup>th</sup> WG 1 meeting, Oct. 2012, resolutions 1, 8, 15, 16, 21*, 26 (N11900).  <i>* appointment of ITU-T SG editor</i>	SoCom (N11470); CSA (N11586); ISACA (N11587); ITU-T SG17 (N11474).	60-day LB/SoV on change TS ->IS (N12077/N12180); Request/endorsement title change (N12145/N12184); Liaisons to: CSA (N11885); ITU-T FG Cloud (N11889); JTC 1/SC 38 (N11899); Meet. report (N12017); DoC (N11915); Text f. 4 <sup>th</sup> WD (N11916).

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

#### Copyright notice

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

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

#### ISO copyright office

Case postale 56 • CH-1211 Geneva 20

Tel. + 41 22 749 01 11

Fax + 41 22 749 09 47

E-mail [copyright@iso.org](mailto:copyright@iso.org)

Web [www.iso.org](http://www.iso.org)

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

Violators may be prosecuted.

ITU-T RECOMMENDATION X.nnnn

INTERNATIONAL STANDARD ISO/IEC 27017

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

## **Summary**

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

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

This Recommendation | International Standard provides controls and implementation guidance for both cloud service providers and for cloud service customers.

# Contents

0	Introduction .....	viii
1	Scope .....	1
2	Normative references .....	1
3	Definitions and abbreviations .....	1
3.1	Terms and definitions .....	1
3.2	Abbreviations .....	2
4	Cloud sector-specific concepts .....	2
4.1	Overview .....	2
4.2	Supplier relationships in cloud services .....	2
4.3	Relationships between cloud service customers and cloud service providers .....	3
4.4	Managing information security risks in cloud services .....	3
4.5	Structure of this standard .....	3
5	Information security policies .....	5
5.1	Management direction for information security .....	5
6	Organization of information security .....	7
6.1	Internal organization .....	7
6.2	Mobile devices and teleworking .....	8
7	Human resource security .....	9
7.1	Prior to employment .....	9
7.2	During employment .....	9
7.3	Termination and change of employment .....	10
8	Asset management .....	11
8.1	Responsibility for assets .....	11
8.2	Information classification .....	12
8.3	Media handling .....	13
9	Access control .....	14
9.1	Business requirements of access control .....	14
9.2	User access management .....	14
9.3	User responsibilities .....	16
9.4	System and application access control .....	16
10	Cryptography .....	19
10.1	Cryptographic controls .....	19
11	Physical and environmental security .....	21
11.1	Secure areas .....	21
11.2	Equipment .....	21
12	Operations security .....	24
12.1	Operational procedures and responsibilities .....	24

12.2	Protection from malware.....	26
12.3	Backup.....	26
12.4	Logging and monitoring .....	27
12.5	Control of operational software .....	29
12.6	Technical vulnerability management .....	29
12.7	Information systems audit considerations .....	30
13	Communications security .....	31
13.1	Network security management.....	31
13.2	Information transfer .....	31
14	System acquisition, development and maintenance.....	33
14.1	Security requirements of information systems .....	33
14.2	Security in development and support processes.....	33
14.3	Test data.....	35
15	Supplier relationships .....	36
15.1	Security in supplier relationship.....	36
15.2	Supplier service delivery management .....	37
16	Information security incident management .....	39
16.1	Management of information security incidents and improvements .....	39
17	Information security aspects of business continuity management.....	42
17.1	Information security continuity .....	42
17.2	Redundancies.....	42
18	Compliance .....	43
18.1	Compliance with legal and contractual requirements.....	43
18.2	Information security reviews .....	44
Annex A	Cloud Service Extended Control Set (normative) .....	46
CLD.6.3	Relationship between cloud service customer and cloud service provider.....	46
CLD.8.1	Responsibility for assets .....	46
CLD.9.5	Access control of cloud service customer's data in shared virtual environment.....	47
CLD.12.1	Operational procedures and responsibilities .....	48
CLD.12.4	Logging and monitoring.....	49
CLD.13.1	Network security management.....	49
Annex B	References on information security risk related cloud computing (informative) .....	51

## Foreword

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating, and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a world-wide basis. The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups that, in turn, produce Recommendations on these topics. The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1. In some areas of information technology that fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

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

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

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

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

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.



## 0 Introduction

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

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

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

## 1 Scope

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

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

This Recommendation | International Standard provides controls and implementation guidance for both cloud service providers and for cloud service customers.

## 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 27000:2014, *Information technology - Security techniques - Information security management systems - Overview and vocabulary*

ISO/IEC 17788, *Information technology – Cloud computing — 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, ISO/IEC 17788 and the following apply.

#### 3.1.1

##### **capability**

quality of being able to perform a given activity

[ISO 19440:2007]

#### 3.1.2

##### **party**

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

[ISO 27729:2012]

## 3.2 Abbreviations

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

IaaS: Infrastructure as a Service

PaaS: Platform as a Service

PII: Personally Identifiable Information

SaaS: Software as a Service

## 4 Cloud sector-specific concepts

### 4.1 Overview

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

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

As an extension to ISO/IEC 27002, this Recommendation | International Standard further provides cloud service specific controls, implementation guidance and other information (see 4.5) which are intended to meet specific risks that accompany the technical and operational features of cloud services (see Annex B). Cloud service customer and cloud service provider can reference ISO/IEC 27002 and this Recommendation | International Standard, and select controls with its implementation guidance from them, and add other controls if necessary. This can be done through the process of information security risk assessment and risk treatment in the organizational and business context where cloud services are used or provided (see 4.4).

### 4.2 Supplier relationships in cloud services

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

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

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

#### **4.3 Relationships between cloud service customers and cloud service providers**

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

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

#### **4.4 Managing information security risks in cloud services**

Cloud service customers and providers should have their information security risk management processes in place. They are advised to refer to ISO/IEC 27001 for the requirements of the risk management in the context of information security management system, and ISO/IEC 27005 for further guidance on the information security risk management. ISO 31000, which ISO/IEC 27001 and ISO/IEC 27005 conform to, can also help general understanding on the risk management.

In contrast to the general applicability of the information security risk management processes, cloud computing has its own types of risk sources, including threats and vulnerabilities, which are derived from its features, e.g. networking, scalability and elasticity of the system, resource sharing, self-service provisioning, administration on demand, cross jurisdictional service provisioning and limited visibility into the implementation of controls. Annex B provides references that give information on these risk sources and associated risks in the use and provisioning of the cloud services.

The controls and implementation guidance given in the clauses 5 to 18 and Annex A of this Recommendation | International Standard address these cloud computing specific risk sources and risks.

#### **4.5 Structure of this standard**

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

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

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

When a control of 27002 or Annex A of this Recommendation | International Standard needs additional cloud service specific implementation guidance related to the control, it is given under the subtitle "Implementation guidance for cloud computing". Cloud service specific implementation guidance and other information are included in all clauses.

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

2 Each main security category contains:

3 a) a control objective stating what is to be achieved;

4 b) one or more controls that can be applied to achieve the control objective.

5 Control descriptions are structured as follows:

6 Control objective of ISO/IEC 27002

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

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

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

11 Sector-specific guidance for cloud services

12 The guidance is provided in one of the following two types:

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

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

17 Type 1

Cloud service customer	Cloud service provider

18

19 Type 2

Cloud service customer	Cloud service provider

20

21 Additional information that may need to be considered is provided under the subtitle “Other information  
22 for cloud computing”.

## 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

##### Implementation guidance for cloud computing

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 provider
<p>A policy for cloud computing should be consistent with the organization's acceptable levels of information security risks for their information and other assets.</p> <p>When defining the policy for cloud computing, the cloud service customer should take the following into account:</p> <ul style="list-style-type: none"><li>— information stored in the cloud computing environment that can be subject to access and management by the cloud service provider;</li><li>— assets maintained in the cloud computing environment, e.g. application programs;</li><li>— processes run on the cloud service;</li><li>— users of the cloud service;</li><li>— cloud service customer administrators with privileges;</li><li>— geographical location of the cloud service provider's organisation and storage facilities.</li></ul>	<p>The cloud service provider should define a policy for provisioning cloud computing services that takes the following into account:</p> <ul style="list-style-type: none"><li>— strategic plan that include baseline security requirements applicable to the design and implementation;</li><li>— risks from authorised insiders;</li><li>— multi-tenancy and customer isolation (including virtualisation);</li><li>— cloud service provider administrative user access matrix;</li><li>— strong access control procedures, e.g. strong authentication, for administrative access to hosted cloud services;</li><li>— acceptable use policy specifically for cloud service provider administrators;</li><li>— communications to customers during change management;</li><li>— virtualisation security (e.g., lifecycle management of VMs, storage and access controls for virtualised images, handling of dormant or offline VMs, snapshots, security of hypervisor, and use of self-service portals);</li><li>— access and protection of cloud service customer data;</li><li>— lifecycle management of cloud service customer accounts.</li></ul>

- 1     **5.1.2 Review of the policies for information security**
- 2     Implementation guidance for cloud computing
- 3     Control 5.1.2 and the associated implementation guidance and other information specified in ISO/IEC
- 4     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

##### Implementation guidance for cloud computing

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
<p>The cloud service customer should review the proposed demarcation of information security responsibilities and confirm if it can accept its responsibilities. Responsibilities of both parties should be stated in the agreement.</p> <p>The cloud service customer should review the proposed demarcation of information security responsibilities and confirm if it can accept its responsibilities. Responsibilities of both parties should be stated in the agreement.</p>	<p>The cloud service provider should define and document the demarcation of responsibilities of cloud service customer, cloud service provider and its suppliers. Where applicable, the cloud service provider should define and document responsibilities of its supplier.</p>

##### Other information for cloud computing

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

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

#### 6.1.2 Segregation of duties

##### Implementation guidance for cloud computing

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

#### 6.1.3 Contact with authorities

##### Implementation guidance for cloud computing

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



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

1

2     **6.1.4 Contact with special interest groups**3     Implementation guidance for cloud computing

4     Control 6.1.4 and the associated implementation guidance and other information specified in ISO/IEC  
5     27002 apply.

6     **6.1.5 Information security in project management**7     Implementation guidance for cloud computing

8     Control 6.1.5 and the associated implementation guidance and other information specified in ISO/IEC  
9     27002 apply.

10    **6.2 Mobile devices and teleworking**

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

12    **6.2.1 Mobile device policy**13    Implementation guidance for cloud computing

14    Control 6.2.1 and the associated implementation guidance and other information specified in ISO/IEC  
15    27002 apply.

16    **6.2.2 Teleworking**17    Implementation guidance for cloud computing

18    Control 6.2.2 and the associated implementation guidance and other information specified in ISO/IEC  
19    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**

##### Implementation guidance for cloud computing

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**

##### Implementation guidance for cloud computing

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**

##### Implementation guidance for cloud computing

Control 7.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

<b>Cloud service customer</b>	<b>Cloud service provider</b>
( no additional implementation guidance )	The cloud service provider should ensure adequate regular screening of its staff holding key administration position for cloud services beyond just initial employment or change of roles or responsibilities.

#### **7.2.2 Information security awareness, education and training**

##### Implementation guidance for cloud computing

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.

<b>Cloud service customer</b>	<b>Cloud service provider</b>
The cloud service customer should add the following items to awareness, education and training programmes for business managers, cloud service administrators, cloud service integrators and cloud service users, including	The cloud service provider should provide education and training for employees and contractors concerning the appropriate handling of a cloud service customer's data and derived data, which can contain information confidential to a cloud service customer and/or be subject to

<p>relevant employees and contractors:</p> <ul style="list-style-type: none"> <li>— standards and procedures for the use of cloud services;</li> <li>— information security risks relating to cloud services and how those risks are managed;</li> <li>— system and network environment risks with the use of cloud services.</li> </ul> <p>Information security awareness, education and training programmes about cloud services should be provided to management and the supervising managers, including those of business units. This supports effective co-ordination of information security activities.</p>	<p>specific limitations on access and use by the cloud service provider.</p>
--	--

1     **7.2.3 Disciplinary process**

2     Implementation guidance for cloud computing

3     Control 7.2.3 and the associated implementation guidance and other information specified in ISO/IEC  
4     27002 apply.

5     **7.3 Termination and change of employment**

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

7     **7.3.1 Termination or change of employment responsibilities**

8     Implementation guidance for cloud computing

9     Control 7.3.1 and the associated implementation guidance and other information specified in ISO/IEC  
10    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

##### Implementation guidance for cloud computing

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

Cloud service customer	Cloud service provider
The inventory of assets should account for information and associated assets stored in the cloud computing environment. The records of the inventory should have indication where the assets are maintained, e.g. identification of the cloud service.	(no additional implementation guidance)

##### Other information for cloud computing

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

#### 8.1.2 Ownership of assets

##### Implementation guidance for cloud computing

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

##### Implementation guidance for cloud computing

Control 8.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
The cloud service customer should request the cloud service provider for its rules for the access and control of the cloud service customer's information.	( no additional implementation guidance )

#### 1      **8.1.4 Return of assets**

##### 2      Implementation guidance for cloud computing

3      Control 8.1.4 and the associated implementation guidance and other information specified in ISO/IEC  
4      27002 apply.

#### 5      **8.2 Information classification**

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

##### 7      **8.2.1 Classification of information**

##### 8      Implementation guidance for cloud computing

9      Control 8.2.1 and the associated implementation guidance and other information specified in ISO/IEC  
10      27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
The cloud service customer should classify information and associated assets maintained in the cloud computing environment in accordance with the information classification scheme adopted by the cloud service customer.	( no additional implementation guidance )

11

##### 12      **8.2.2 Labelling of information**

##### 13      Implementation guidance for cloud computing

14      Control 8.2.2 and the associated implementation guidance and other information specified in ISO/IEC  
15      27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
( no additional implementation guidance )	<p>The cloud service provider should document and disclose service functionality allowing cloud service customers to classify and label their information and associated assets.</p> <p>The cloud service customer should label information and associated assets maintained in the cloud computing environment in accordance with the procedures for labelling. Where applicable, functionality of the cloud service supporting the labelling can be adopted.</p>

##### 16      **8.2.3 Handling of assets**

##### 17      Implementation guidance for cloud computing

18      Control 8.2.3 and the associated implementation guidance and other information specified in ISO/IEC  
19      27002 apply.

1    **8.3   Media handling**

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

3    **8.3.1   Management of removable media**

4    Implementation guidance for cloud computing

5    Control 8.3.1 and the associated implementation guidance and other information specified in ISO/IEC  
6    27002 apply.

7    **8.3.2   Disposal of media**

8    Implementation guidance for cloud computing

9    Control 8.3.2 and the associated implementation guidance and other information specified in ISO/IEC  
10   27002 apply.

11   **8.3.3   Physical media transfer**

12   Implementation guidance for cloud computing

13   Control 8.3.3 and the associated implementation guidance and other information specified in ISO/IEC  
14   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

Implementation guidance for cloud computing

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

Implementation guidance for cloud computing

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

Cloud service customer	Cloud service provider
The policy for the use of network services should include requirements for network access for each cloud service.	( no additional implementation guidance )

### 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

Implementation guidance for cloud computing

Control 9.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
( no additional implementation guidance )	For the purpose of access to cloud services, a cloud service provider should provide user registration and de-registration functions and specifications to the cloud service customer.

#### 9.2.2 User access provisioning

Implementation guidance for cloud computing

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

Cloud service customer	Cloud service provider
( no additional implementation guidance )	A cloud service provider should provide functions and specifications for managing the access rights of a cloud service customer.

1

## 2 Other information for cloud computing

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

## 8 **9.2.3 Management of privileged access rights**

### 9 Implementation guidance for cloud computing

10 Control 9.2.3 and the associated implementation guidance and other information specified in ISO/IEC  
11 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
The cloud service customer should use strong authentication techniques (e.g. multi-factor-authentication) for authenticating cloud service administrators to the administration capabilities of a cloud service.	The cloud service provider should provide strong authentication techniques for authenticating customer cloud service administrators to the administration capabilities of a cloud service. For example, the cloud service provider should provide multi-factor authentication capabilities or enable the use of 3rd party multi-factor authentication mechanisms.

12

## 13 Other information for cloud computing

14 Virtual systems, cloud service customer data, virtual resources and other assets can be modified,  
15 corrupted, deleted or disabled through the use of the administration capabilities associated with a  
16 cloud service. Unauthorized use of these administration capabilities can have major impacts on the  
17 availability, confidentiality and integrity of the cloud service.

## 18 **9.2.4 Management of secret authentication information of users**

### 19 Implementation guidance for cloud computing

20 Control 9.2.4 and the associated implementation guidance and other information specified in ISO/IEC  
21 27002 apply. The following sector-specific guidance also applies.



Cloud service customer	Cloud service provider
The cloud service customer should confirm that the management procedure of allocating the secret authentication information such as password specified by the cloud service meets the requirement of the cloud service customer.	The cloud service provider should provide information on procedures for the management of secret authentication information of the cloud service customer, including procedures for distribution of such information and procedures for user authentication.

1

2 Other information for cloud computing

3 It is recommended that the management of secret authentication information be under the control of  
4 the cloud service customer, through the use of third party Identity and Access Management  
5 technologies.

6 **9.2.5 Review of user access rights**7 Implementation guidance for cloud computing

8 Control 9.2.5 and the associated implementation guidance and other information specified in ISO/IEC  
9 27002 apply.

10 **9.2.6 Removal or adjustment of access rights**11 Implementation guidance for cloud computing

12 Control 9.2.6 and the associated implementation guidance and other information specified in ISO/IEC  
13 27002 apply.

14 **9.3 User responsibilities**

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

16 **9.3.1 Use of secret authentication information**17 Implementation guidance for cloud computing

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

20 **9.4 System and application access control**

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

22 **9.4.1 Information access restriction**23 Implementation guidance for cloud computing

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

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

1

## 2 Other information for cloud computing

3 The cloud computing environment brings some additional areas that need to be controlled for access.  
4 As part of the cloud service or cloud service functions, access to items such as the hypervisor  
5 management functions and administrative consoles, can need additional access control.

## 6 **9.4.2 Secure log-on procedures**

### 7 Implementation guidance for cloud computing

8 Control 9.4.2 and the associated implementation guidance and other information specified in ISO/IEC  
9 27002 apply.

## 10 **9.4.3 Password management system**

### 11 Implementation guidance for cloud computing

12 Control 9.4.3 and the associated implementation guidance and other information specified in ISO/IEC  
13 27002 apply.

## 14 **9.4.4 Use of privileged utility programs**

### 15 Implementation guidance for cloud computing

16 Control 9.4.4 and the associated implementation guidance and other information specified in ISO/IEC  
17 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
The cloud service customer should identify the utility programs to be used in the cloud computing environment and ensure that they do not interfere with the controls of the cloud service.	<p>The cloud service provider should identify the requirements for any utility programs used within the cloud service environment and ensure that the cloud service customer meets these requirements.</p> <p>The cloud service provider should ensure that no utility programs capable of overriding system and application controls should be run in the cloud environment without permission from the cloud service customer.</p>

18

- 1     **9.4.5 Access control to program source code**
- 2     Implementation guidance for cloud computing
- 3     Control 9.4.5 and the associated implementation guidance and other information specified in ISO/IEC
- 4     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

##### Implementation guidance for cloud computing

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

Cloud service customer	Cloud service provider
<p>The cloud service customer should require cryptographic controls for a cloud service that cannot be compromised by the cloud service provider or any other party, whether those controls are supplied by the customer or by the provider.</p> <p>In case that the cloud service provider offers cryptography, the cloud service customer should request information from the cloud service provider to confirm that the cryptographic functionalities:</p> <ul style="list-style-type: none"><li>— meet the requirements of the customer's policy;</li><li>— are compatible with the cryptographic protection that will be used by the cloud service customer;</li><li>— apply to data being transferred to and from the cloud service, as well as for data stored within the cloud service.</li></ul>	<p>The cloud service provider should provide information regarding its cryptographic functionalities available to the cloud service customer.</p>

#### 10.1.2 Key management

##### Implementation guidance for cloud computing

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

Cloud service customer	Cloud service provider
<p>The cloud service customer should identify the cryptographic keys it needs to manage with each cloud service, and implement procedures for key management.</p> <p>Where the cloud service itself has key</p>	<p>If the cloud service provider offers capabilities for the cloud service customer to independently store and manage encryption keys used for the protection of cloud service customer data, the cloud service provider should provide information on its key management service to the cloud</p>

<p>management functionality, the cloud service customer should request the following information on the procedures used to manage keys related to cloud service:</p> <ul style="list-style-type: none"> <li>— type of keys;</li> <li>— specifications of the key management system, including procedures for each stage of the key life-cycle, i.e. generating, changing or updating, storing, retiring, retrieving, retaining and destroying;</li> <li>— recommended key management procedures for use by the customer.</li> </ul>	<p>service customer, including but not restricted to:</p> <ul style="list-style-type: none"> <li>— type of keys;</li> <li>— specifications of the key management system, including procedures for generating, changing or updating, storing, retiring, retrieving, retaining and destroying of keys;</li> <li>— recommended key management procedures to be used by the cloud service customer;</li> <li>— Status of keys (e.g. valid, revoked or destroyed).</li> </ul> <p>The cloud service provider should provide a mechanism for the protection of encrypted information during transmission and storage as the possibility of key disclosure is very high due to cloud multi-tenancy. Strict key security should be enforced and the use of multiple keys for different VM would reduce the exposure in case any one key is compromised.</p>
---	--

1

2 Other information for cloud computing

3 The cloud service customer should not permit the cloud service provider to store and manage  
4 encryption keys for cryptographic operations that are performed using equipment that is on customer  
5 controlled sites, and outside the scope of services provided by cloud service provider. The cloud  
6 service customer should employ a separate and distinct service to store and manage these 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**

Implementation guidance for cloud computing

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

#### **11.1.2 Physical entry controls**

Implementation guidance for cloud computing

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**

Implementation guidance for cloud computing

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**

Implementation guidance for cloud computing

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**

Implementation guidance for cloud computing

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**

Implementation guidance for cloud computing

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.

1     **11.2.1 Equipment siting and protection**

2     Implementation guidance for cloud computing

3     Control 11.2.1 and the associated implementation guidance and other information specified in ISO/IEC  
4     27002 apply.

5     **11.2.2 Supporting utilities**

6     Implementation guidance for cloud computing

7     Control 11.2.2 and the associated implementation guidance and other information specified in ISO/IEC  
8     27002 apply.

9     **11.2.3 Cabling security**

10    Implementation guidance for cloud computing

11    Control 11.2.3 and the associated implementation guidance and other information specified in ISO/IEC  
12    27002 apply.

13    **11.2.4 Equipment maintenance**

14    Implementation guidance for cloud computing

15    Control 11.2.4 and the associated implementation guidance and other information specified in ISO/IEC  
16    27002 apply.

17    **11.2.5 Removal of assets**

18    Implementation guidance for cloud computing

19    Control 11.2.5 and the associated implementation guidance and other information specified in ISO/IEC  
20    27002 apply.

21    **11.2.6 Security of equipment and assets off-premises**

22    Implementation guidance for cloud computing

23    Control 11.2.6 and the associated implementation guidance and other information specified in ISO/IEC  
24    27002 apply.

25    **11.2.7 Secure disposal or re-use of equipment**

26    Implementation guidance for cloud computing

27    Control 11.2.7 and the associated implementation guidance and other information specified in ISO/IEC  
28    27002 apply. The following sector-specific guidance also applies.

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

1

2     **11.2.8 Unattended user equipment**

3     Implementation guidance for cloud computing

4     Control 11.2.8 and the associated implementation guidance and other information specified in ISO/IEC  
5     27002 apply.

6     **11.2.9 Clear desk and clear screen policy**

7     Implementation guidance for cloud computing

8     Control 11.2.9 and the associated implementation guidance and other information specified in ISO/IEC  
9     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**Implementation guidance for cloud computing

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

**12.1.2 Change management**Implementation guidance for cloud computing

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

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

**12.1.3 Capacity management**Implementation guidance for cloud computing

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

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

## Other information for cloud computing

Cloud services involve resources – software, processing hardware, data storage, network connectivity – that are under the control of the cloud service provider and made available to the cloud service customer under the terms of the master service agreement and a related SLA. It is typical for cloud services to provide capacity of the associated resources in an elastic, scalable form, provided to the customer on demand.

However, in many cases, the resources provided can have capacity constraints and it is necessary for the cloud service customer to be aware of these constraints. Examples of capacity constraints include:

- for processing resources, the number of processor cores available to an application may be limited, the power of each processor core may be limited;
- for processing resources, the maximum amount of RAM available to an application may be limited;
- for processing resources, there may be an upper bound to the total number of virtual machines that can be active at one time;
- for data storage resources, there may be upper bounds to:
  - the total amount of storage available;
  - the maximum size of a single file / object which can be stored;
  - the maximum amount of data available on a particular logical volume.
- for data storage resources, there may be limits to the rate at which data can be read from or written to the storage;
- for network connectivity, there may be upper bounds to the bandwidth available or to the number of simultaneous connections;
- for software resources, there may be limits to the latency of requests, the number of simultaneous users, the transaction throughput;
- the lead time to add additional capacity is another constraint which can impact the customer;

The constraints may vary depending on the particular cloud service or the particular subscription that the cloud service customer chooses to purchase. If the cloud service customer has requirements that

1 exceed the constraints, the customer may need to change the cloud service or change the  
2 subscription.

3 In order for the customer to perform capacity management for cloud services, the customer must have  
4 access to relevant statistics on resource usage:

5 — statistics for particular time periods;

6 — maximum levels of resource usage.

#### 7 **12.1.4 Separation of development, testing and operational environments**

##### 8 Implementation guidance for cloud computing

9 Control 12.1.4 and the associated implementation guidance and other information specified in ISO/IEC  
10 27002 apply.

### 11 **12.2 Protection from malware**

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

#### 13 **12.2.1 Controls against malware**

##### 14 Implementation guidance for cloud computing

15 Control 12.2.1 and the associated implementation guidance and other information specified in ISO/IEC  
16 27002 apply.

### 17 **12.3 Backup**

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

#### 19 **12.3.1 Information backup**

##### 20 Implementation guidance for cloud computing

21 Control 12.3.1 and the associated implementation guidance and other information specified in ISO/IEC  
22 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
Where backup capability is provided by the cloud service provider as part of the cloud service, the cloud service customer should request the specifications of the backup capability from the cloud service provider and should verify that they meet the backup requirements of the cloud service customer.	The cloud service provider should provide the specifications of its backup capabilities to the cloud service customer. The specifications should include the following information, (as appropriate):
Where no backup capability is provided as part of the cloud service, then the cloud service customer is responsible for handling backups according to clause 12.3.1 of ISO 27002.	— scope and schedule of backups;
NOTE: Varying levels of backup and restore may can be offered as a service at additional cost and	— backup methods and data formats (including encryption, if relevant);
	— retention periods for backup data;
	— procedures for verifying integrity of backup data;

cloud service customers may choose what and when to backup.	<ul style="list-style-type: none"> <li>— procedures and timescales involved in restoring data from backup;</li> <li>— procedures to test the backup capabilities;</li> <li>— storage location of backups.</li> </ul> <p>The cloud service provider should provide secure and segregated access to backups, such as virtual snapshots, if such service is offered to cloud service customers.</p>
---	--

1

## 2 **12.4 Logging and monitoring**

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

### 4 **12.4.1 Event logging**

#### 5 Implementation guidance for cloud computing

6 Control 12.4.1 and the associated implementation guidance and other information specified in ISO/IEC  
7 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
<p>The cloud service customer should request from the cloud service provider the specifications of the event logs of the cloud service customer produced and retained by the cloud service provider, in relation to a cloud service and its associated resources:</p> <ul style="list-style-type: none"> <li>— the types of log records;</li> <li>— the retention periods which apply to each type of record;</li> <li>— the rights the customer has to inspect log records and the procedures for inspecting log records.</li> </ul> <p>For logging information that is produced by software controlled by the cloud service customer running in a cloud service (e.g. IaaS or PaaS service), the customer should ensure that logging information is written to permanent, non-volatile storage that can be accessed by the customer at a later point in time.</p>	<p>The cloud service customer should request from the cloud service provider the specifications of the event logs of the cloud service customer produced and retained by the cloud service provider, in relation to a cloud service and its associated resources:</p> <ul style="list-style-type: none"> <li>— the types of log records;</li> <li>— the retention periods which apply to each type of record;</li> <li>— the rights the customer has to inspect log records and the procedures for inspecting log records.</li> </ul> <p>Where a cloud service customer is permitted to access log records controlled by the cloud service provider, the provider should ensure that the customer can only access records that relate to that customer's activities, and cannot access any log records which relate to the activities of other cloud service customers.</p> <p>Cloud service provider should record event logs proving Service Level Agreement fulfilment. The provider should have documented procedures for sharing such logs and ensuring that the information contained in</p>

	such logs is sacrosanct.
--	--------------------------

## Other information for cloud computing

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

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

The responsibility for logging will vary depending on the type of cloud service being used. A cloud service provider's logging responsibility can be limited to cloud computing infrastructure components and the cloud service customer is responsible for logging their own virtual machines and applications.

### **12.4.2 Protection of log information**

#### Implementation guidance for cloud computing

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**

#### Implementation guidance for cloud computing

Control 12.4.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
If a privileged operation in the cloud computing environment is delegated to the cloud service customer, the operations of the cloud service customer should be logged.	If the cloud service customer is given access to privileged operations related to a cloud service, all use of those privileged operations should be recorded in a secure operation log.

## Other information for cloud computing

Demarcation of responsibility between the cloud service customer and the cloud service provider (see 6.1.1) should cover that of the privileged operation in the cloud service as needed. Monitoring and logging of the privileged operation are the measures of preventive and corrective actions against incorrect operation that can have adverse effect on the cloud service not limited to the cloud service customer's environment.

## 12.4.4 Clock synchronisation

### Implementation guidance for cloud computing

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

Cloud service customer	Cloud service provider
( no additional implementation guidance )	The cloud service provider should provide the information regarding clock synchronization for use of clock synchronization with the other systems of the cloud service customer.

## 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

#### Implementation guidance for cloud computing

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

## 12.6 Technical vulnerability management

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

### 12.6.1 Management of technical vulnerabilities

#### Implementation guidance for cloud computing

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
The cloud service customer should request information from the cloud service provider about technical vulnerability management as it applies to the cloud service and the resources it uses.	<p>The cloud service provider should make cloud service customers aware that a well-defined vulnerability management process exists. This can be validated by self assessment or by a 3rd party assessor.</p> <p>The information provided should describe the provider's approach to the points made in the guidance contained in clause 12.6.1 of ISO 27002.</p>

### 12.6.2 Restrictions on software installation

#### Implementation guidance for cloud computing

1 Control 12.6.2 and the associated implementation guidance and other information specified in ISO/IEC  
2 27002 apply.

3 **12.7 Information systems audit considerations**

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

5 **12.7.1 Information systems audit controls**

6 Implementation guidance for cloud computing

7 Control 12.7.1 and the associated implementation guidance and other information specified in ISO/IEC  
8 27002 apply.

9

## 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

##### Implementation guidance for cloud computing

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

#### 13.1.2 Security of network services

##### Implementation guidance for cloud computing

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

#### 13.1.3 Segregation in networks

##### Implementation guidance for cloud computing

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
<p>When using IaaS, the cloud service customer should define the requirements for segregating networks for multi-tenant access restrictions and verify that the cloud service provider meets those requirements.</p> <p>Where appropriate, the cloud service customer should periodically verify that the cloud service provider is enforcing logical segregation of network access. This requirement should be documented in an agreement between the customer and the provider.</p>	<p>The cloud service provider should enforce physical segregation of network access for the following:</p> <ul style="list-style-type: none"><li>— separation of each tenancy in a multi-tenant cloud service;</li><li>— separation of the cloud service provider's internal administration from the customer's cloud computing environment or any other unauthorized users.</li></ul> <p>Where appropriate, the cloud service provider should assist the cloud service customer in the verification of the logical segregation implemented by the provider</p>

##### Other information for cloud computing

Laws and regulations can require the segregation of networks or the isolation of network traffic.

### 13.2 Information transfer

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



1     **13.2.1 Information transfer policies and procedures**

2     Implementation guidance for cloud computing

3     Control 13.2.1 and the associated implementation guidance and other information specified in ISO/IEC  
4     27002 apply.

5     **13.2.2 Agreements on information transfer**

6     Implementation guidance for cloud computing

7     Control 13.2.2 and the associated implementation guidance and other information specified in ISO/IEC  
8     27002 apply.

9     **13.2.3 Electronic messaging**

10    Implementation guidance for cloud computing

11    Control 13.2.3 and the associated implementation guidance and other information specified in ISO/IEC  
12    27002 apply.

13    **13.2.4 Confidentiality or non-disclosure agreements**

14    Implementation guidance for cloud computing

15    Control 13.2.4 and the associated implementation guidance and other information specified in ISO/IEC  
16    27002 apply.

17

## **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**

##### Implementation guidance for cloud computing

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.

<b>Cloud service customer</b>	<b>Cloud service provider</b>
<p>The cloud service customer should determine their security requirements for the cloud service and then evaluate whether or not services offered by a cloud service provider can meet these requirements.</p> <p>For the evaluation, the cloud service customer should obtain from the cloud service provider the service specifications that include information security specifications.</p> <p>Where applicable, the cloud service customer should obtain from the cloud service provider a description of the information security controls implemented by the provider.</p>	<p>Where the cloud service provider offers public cloud services using multi-tenancy, there is a need for information security controls to ensure isolation of different tenants.</p> <p>The cloud service provider should enforce isolation between the activities of cloud service customers using cloud services and the internal systems and operations of the cloud service provider.</p> <p>The cloud service provider should provide information to cloud service customers about the security controls which apply to the cloud services they use. This information should be designed to be informative without divulging information that could be useful to someone with malicious intent.</p>

#### **14.1.2 Securing applications services on public networks**

##### Implementation guidance for cloud computing

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**

##### Implementation guidance for cloud computing

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**

##### Implementation guidance for cloud computing

- 1 Control 14.2.1 and the associated implementation guidance and other information specified in ISO/IEC  
2 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
The cloud service customer should request information from the cloud service provider about the use of secure development procedures and practices.	The cloud service provider should provide information about their use of secure development procedures and practices. For example, such as those in 27034-1.

3

#### 4 **14.2.2 System change control procedures**

##### 5 Implementation guidance for cloud computing

- 6 Control 14.2.2 and the associated implementation guidance and other information specified in ISO/IEC  
7 27002 apply.

#### 8 **14.2.3 Technical review of applications after operating platform changes**

##### 9 Implementation guidance for cloud computing

- 10 Control 14.2.3 and the associated implementation guidance and other information specified in ISO/IEC  
11 27002 apply.

#### 12 **14.2.4 Restrictions on changes to software packages**

##### 13 Implementation guidance for cloud computing

- 14 Control 14.2.4 and the associated implementation guidance and other information specified in ISO/IEC  
15 27002 apply.

#### 16 **14.2.5 Secure system engineering principles**

##### 17 Implementation guidance for cloud computing

- 18 Control 14.2.5 and the associated implementation guidance and other information specified in ISO/IEC  
19 27002 apply.

#### 20 **14.2.6 Secure development environment**

##### 21 Implementation guidance for cloud computing

- 22 Control 14.2.6 and the associated implementation guidance and other information specified in ISO/IEC  
23 27002 apply.

#### 24 **14.2.7 Outsourced development**

##### 25 Implementation guidance for cloud computing

- 26 Control 14.2.7 and the associated implementation guidance and other information specified in ISO/IEC  
27 27002 apply.

1     **14.2.8 System security testing**

2     Implementation guidance for cloud computing

3     Control 14.2.8 and the associated implementation guidance and other information specified in ISO/IEC  
4     27002 apply.

5     **14.2.9 System acceptance testing**

6     Implementation guidance for cloud computing

7     Control 14.2.9 and the associated implementation guidance and other information specified in ISO/IEC  
8     27002 apply.

9     Other information for cloud computing

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

12    **14.3 Test data**

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

14    **14.3.1 Protection of test data**

15    Implementation guidance for cloud computing

16    Control 14.3.1 and the associated implementation guidance and other information specified in ISO/IEC  
17    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

##### Implementation guidance for cloud computing

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 customer	Cloud service provider
The cloud service customer should include the cloud service provider as a type of supplier in their information security policy for supplier relationships. This will help to mitigate risks associated with the cloud service provider's access to and management of the cloud service customer's information.	( no additional implementation guidance )

#### 15.1.2 Addressing security within supplier agreements

##### Implementation guidance for cloud computing

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

<ul style="list-style-type: none"> <li>— auditing;</li> <li>— collection, maintenance and protection of evidence, including logs and audit trails;</li> <li>— protection of information upon termination of service agreement;</li> <li>— authentication and access control;</li> <li>— identity and access management.</li> </ul>	<ul style="list-style-type: none"> <li>— collection of evidence;</li> <li>— technical compliance checking;</li> <li>— security testing;</li> <li>— auditing;</li> <li>— collection, maintenance and protection of evidence, including logs and audit trails;</li> <li>— protection of information upon termination of service agreement;</li> <li>— authentication and access control;</li> <li>— identity and access management.</li> </ul> <p>When the cloud service provider provides cloud services based on a supply chain, the cloud service provider should provide risk management objectives to suppliers and request each of the suppliers to perform risk management activities to achieve the objectives.</p>
--	---

1

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

### 3     Implementation guidance for cloud computing

4     Control 15.1.3 and the associated implementation guidance and other information specified in ISO/IEC  
5     27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
( no additional implementation guidance )	If a cloud service provider is a cloud service customer of other services, the cloud service provider should ensure service levels to cloud service customers are maintained or exceeded.

6

## 7     **15.2 Supplier service delivery management**

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

### 9     **15.2.1 Monitoring and review of supplier services**

#### 10    Implementation guidance for cloud computing

11    Control 15.2.1 and the associated implementation guidance and other information specified in ISO/IEC  
12    27002 apply.

- 1     **15.2.2 Managing changes to supplier services**
- 2     Implementation guidance for cloud computing
- 3     Control 15.2.2 and the associated implementation guidance and other information specified in ISO/IEC
- 4     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

##### Implementation guidance for cloud computing

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

Cloud service customer	Cloud service provider
The cloud service customer should verify the demarcation of responsibility on the management of information security incidents and should ensure that it is sufficient to meet the requirements of the cloud service customer.	<p>Regarding to the management of information security incidents, the cloud service provider should define the scope of responsibility and should specify the responsibility of cloud service customer.</p> <p>The cloud service provider should consider the following:</p> <ul style="list-style-type: none"><li>— scope of information security incidents which the cloud provider deals with;</li><li>— level of disclosure on detection and response of information security incidents;</li><li>— timing to notify the detection of information security incidents;</li><li>— procedure for the notification of information security incidents;</li><li>— contacts that handles the issues related to information security incidents;</li><li>— the presence or absence of compensation about the information security incidents.</li></ul>

#### 16.1.2 Reporting information security events

##### Implementation guidance for cloud computing

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

Cloud Service Customer	Cloud Service Provider
The cloud service customer should get	The cloud service provider should provide



information from the cloud service provider about:	mechanisms for:
<ul style="list-style-type: none"> <li>— the mechanism by which the cloud service customer can report information security events it has discovered to the cloud service provider;</li> <li>— the mechanism by which the cloud service provider can report security events it has discovered to the cloud service customer;</li> <li>— the mechanism by which the cloud service customer can track what is happening in relation to a reported information security event.</li> </ul>	<ul style="list-style-type: none"> <li>— a cloud service customer to report an information security event to the provider;</li> <li>— the cloud service provider to report an information security event to a cloud service customer;</li> <li>— the customer to track what is happening in relation to a reported information security event.</li> </ul>

1

2 Other information for cloud computing

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

6 **16.1.3 Reporting information security weaknesses**7 Implementation guidance for cloud computing

8 Control 16.1.3 and the associated implementation guidance and other information specified in ISO/IEC  
9 27002 apply.

10 **16.1.4 Assessment of and decision on information security events**11 Implementation guidance for cloud computing

12 Control 16.1.4 and the associated implementation guidance and other information specified in ISO/IEC  
13 27002 apply.

14 **16.1.5 Response to information security incidents**15 Implementation guidance for cloud computing

16 Control 16.1.5 and the associated implementation guidance and other information specified in ISO/IEC  
17 27002 apply.

18 **16.1.6 Learning from information security incidents**19 Implementation guidance for cloud computing

20 Control 16.1.6 and the associated implementation guidance and other information specified in ISO/IEC  
21 27002 apply.

22 **16.1.7 Collection of evidence**23 Implementation guidance for cloud computing

- 1 Control 16.1.7 and the associated implementation guidance and other information specified in ISO/IEC  
2 27002 apply. The following sector-specific guidance also applies.

Cloud service customer	Cloud service provider
The cloud service customer and the cloud service provider should identify the policies and procedures required to respond to requests for evidence of information within the cloud computing environment. Specifically, restrictions on acquisition of evidence should be identified by the cloud service customer and the cloud service provider.	

3

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

2    **17.1 Information security continuity**

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

4    **17.1.1 Planning information security continuity**

5    Implementation guidance for cloud computing

6    Control 17.1.1 and the associated implementation guidance and other information specified in ISO/IEC  
7    27002 apply.

8    **17.1.2 Implementing information security continuity**

9    Implementation guidance for cloud computing

10   Control 17.1.2 and the associated implementation guidance and other information specified in ISO/IEC  
11   27002 apply.

12   **17.1.3 Verify, review and evaluate information security continuity**

13   Implementation guidance for cloud computing

14   Control 17.1.3 and the associated implementation guidance and other information specified in ISO/IEC  
15   27002 apply.

16   **17.2 Redundancies**

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

18   **17.2.1 Availability of information processing facilities**

19   Implementation guidance for cloud computing

20   Control 17.2.1 and the associated implementation guidance and other information specified in ISO/IEC  
21   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

##### Implementation guidance for cloud computing

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

Cloud service customer	Cloud service provider
<p>The cloud service customer should identify relevant legal, regulatory and contractual requirements and ensure compliance with them. Relevant laws and regulations can be those of the jurisdictions governing the cloud service customer or the cloud service provider.</p> <p>The cloud service customer should identify relevant standards, e.g. those of financial, healthcare or other sectors, required for the cloud service customer's business, and have evidence about the compliance of the cloud service provider. For example, the standard can require third party auditing on the information systems which can or cannot be acceptable for the cloud service provider.</p>	<p>The cloud service provider should assist the cloud service customer in its efforts to identify the applicable jurisdictions where the cloud services are operated and/or provided, and which are applicable to the cloud service provider and the information he hosts.</p> <p>The cloud service provider should identify the extent to which its services meet the relevant legal requirements (e.g., regarding the use of encryption to protect PII). It should also clearly identify any legal requirements that its services do not meet. This information should be provided to the cloud service customer when requested.</p> <p>The cloud service provider should provide the cloud service customer with evidence of their current certifications for specific regulations and compliance requirements.</p>

##### Other information for cloud computing

The legal and regulatory requirements which apply to the use and the provisioning of cloud services should be identified, particularly where the processing, storage and communication capabilities are geographically distributed and multiple jurisdictions are involved. Examples where legal and regulatory requirements can vary depending on the jurisdiction include the encryption of information and the protection of PII.

It is important to note that compliance requirements, whether legal or contractual, remain the responsibility of the cloud service customer. Compliance responsibilities cannot be outsourced or transferred to the cloud service provider.

#### 18.1.2 Intellectual property rights (IPR)

##### Implementation guidance for cloud computing

Control 18.1.2 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
Installing commercially licensed software into a cloud service could cause a breach of the license terms for the software. The cloud service customer should have a procedure for checking the license terms before permitting any licensed software to be installed into a cloud service. Particular attention should be paid to cases where the cloud service is elastic and scalable and where the software might be run on more systems or on more processors than the license permits.	If the cloud service provider provides the backup capabilities to the cloud service customer, the cloud service provider should confirm with the cloud service customer that the backup remains in scope of the intellectual property rights of the cloud service customer, and should identify that the cloud service customer accept its responsibility when the backup breaches the intellectual property rights.

### 18.1.3 Protection of records

#### Implementation guidance for cloud computing

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

#### Implementation guidance for cloud computing

Control 18.1.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. ISO/IEC 27018, Code of practice for PII protection in public clouds acting as PII processors, offers additional information on this topic.

### 18.1.5 Regulation of cryptographic controls

#### Implementation guidance for cloud computing

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

Cloud service customer	Cloud service provider
The cloud service customer should define the cryptographic controls required for regulatory compliance and verify that the cloud service meets those requirements.	The cloud service provider should provide to the cloud service customer, descriptions of the cryptographic controls implemented by the provider.

## 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

#### Implementation guidance for cloud computing

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

Cloud service customer	Cloud service provider
<p>The cloud service customer should seek assurance in the form of documented evidence from the cloud service provider, related to for the implementation of information security guidelines and controls as claimed by the cloud service provider.</p>	<p>The cloud service provider should provide documented evidence to cloud service customer to substantiate its claim of implementing information security guidelines and controls.</p> <p>In cases where individual cloud service customer audits are impractical or may increase risks to information security, the cloud service provider should make available to prospective cloud service customers, prior to entering into a contract, independent evidence that information security is implemented and operated in accordance with the cloud service provider's policies and procedures. A relevant independent audit as selected by the cloud service provider should normally be an acceptable method for fulfilling the cloud service customer's interest in reviewing the cloud service provider's operations, provided sufficient transparency is provided.</p>

1      **18.2.2 Compliance with security policies and standards**

2      Implementation guidance for cloud computing

3      Control 18.2.2 and the associated implementation guidance and other information specified in ISO/IEC  
4      27002 apply.

5      **18.2.3 Technical compliance review**

6      Implementation guidance for cloud computing

7      Control 18.2.3 and the associated implementation guidance and other information specified in ISO/IEC  
8      27002 apply.

## Annex A

### Cloud Service Extended Control Set

(normative)

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

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

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

[Editor's note: JP will propose new text for this section]

#### CLD.8.1 Responsibility for assets

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

##### CLD.8.1.5 Removal of assets

[Editor's note: the editors request suggestions for a different title for this control.]

##### Control

Assets for the cloud service customer should be removed in a timely manner upon termination of use of a cloud service.

##### Implementation guidance for cloud computing

Cloud service customer	Cloud service provider
<p>The cloud service customer should ensure that arrangements are made for the removal of their assets upon termination of use of a cloud service.</p> <p>The asset removal arrangements should be documented in an agreement and should be performed in a timely manner. The arrangements should include the types of assets to be removed.</p>	<p>The cloud service provider should provide information about the arrangements for the removal of the cloud service customer's assets upon termination of use of a cloud service.</p> <p>The asset removal arrangements should be documented in an agreement and should be performed in a timely manner. The arrangements should include the types of assets to be removed.</p> <p>Where relevant, logs and audit trails maintained by the cloud service provider that are required to be archived as part of the record retention policy or because of requirements to retain as evidences should also be returned along with other assets or should be made available by the cloud service</p>

	provider upon request.
--	------------------------

## 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 Segregation in virtual computing environments

#### Control

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

#### Implementation guidance for cloud computing

Cloud service customer	Cloud service provider
( no additional implementation guidance )	<p>The cloud service provider should enforce logical segregation of virtualized applications, operating systems, storage, and networks for the following:</p> <ul style="list-style-type: none"> <li>— separation of cloud service customers in multi-tenant environments;</li> <li>— separation of the cloud service provider's internal administration from the cloud service customers' virtual environments.</li> </ul> <p>The cloud service provider should restrict the use of customer-supplied software in the virtual environment that can override the protection of virtual environments for other cloud service customers.</p>

#### Other information for cloud computing

Implementation of the logical segregation depends upon the technologies applied to the virtualization:

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

— When a 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".

Secure multi-tenancy and related guidance given in "ISO/IEC 27040, Information technology – Security techniques – Storage security" can be applicable to the cloud computing environment.



1 **CLD.9.5.2 Virtual Machine Hardening**2 Control

3 Virtual machines in a cloud computing environment should be hardened to meet business needs.

4 Implementation guidance for cloud computing

Cloud service customer	Cloud service provider
When using virtual machines, ensure that all aspects are hardened (only those ports, protocols and services that are need to run the cloud service are enabled) and the appropriate technical controls are in place (e.g. anti-malware, logging) for each virtual machine used.	

5

6 **CLD.12.1 Operational procedures and responsibilities**

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

8 **CLD 12.1.5 Administrator's operational security**9 Control10 Procedures for administrative operations of a cloud computing environment should be defined,  
11 documented and monitored.12 Implementation guidance for cloud computing

Cloud service customer	Cloud service provider
<p>The cloud service customer should document procedures for critical operations where a failure can cause unrecoverable damage to assets in the cloud computing environment. These operations should be performed and monitored by a supervisor.</p> <p>Examples of the critical operations are:</p> <ul style="list-style-type: none"> <li>— installation, changes, and deletion of virtualized devices such as servers, networks and storage;</li> <li>— termination procedures for cloud service usage;</li> <li>— backup and restoration.</li> </ul>	( no additional implementation guidance )

13

14 Other information for cloud computing:

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

#### **CLD.12.4 Logging and monitoring**

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

##### **CLD.12.4.5 Monitoring of Cloud Services**

###### Control

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

###### Implementation guidance for cloud computing

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

#### **CLD.13.1 Network security management**

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

##### **CLD.13.1.4 Consistency between virtual and physical networks**

###### Control

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

1 Implementation guidance for cloud computing

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

2

3 Other information for cloud computing

4 In a cloud computing environment built on virtualization technology, a virtual network is configured on  
5 virtual infrastructure on a physical network. In such environments, inconsistency of network policies  
6 can cause system outages or access control violations.

7 NOTE: Depending on the type of cloud service, the level of responsibility for virtual network  
8 configurations may vary between a cloud service customer and a cloud service provider.

## Annex B

### References on information security risk related cloud computing (informative)

Proper use of the information security controls provided by this Recommendation | International Standard relies on the organization's information security risk assessment and treatment. Although these are important subjects, the focus of this Recommendation | International Standard is not on the approach of information security risk assessment and treatment. Following is a list of references that include descriptions on the risk sources and risks in the use and provisioning of cloud services. It should be noted that risk sources and risks vary according to the type and nature of the service and the emerging technologies of cloud computing. Users of this Recommendation | International Standard are recommended to refer to the current versions of the documents as necessary.

**[Editor's note: NBs and liaisons are requested to provide additional references for this list].**

- NIST, SP800-144 Guidelines on Security and Privacy in Public Cloud Computing - Dec. 2011
- NIST, SP800-145 The NIST Definition of Cloud Computing - Sep. 2011
- NIST, SP800-146 Cloud Computing Synopsis and Recommendations - May 2012
- NIST, SP500-291 NIST Cloud Computing Standards Roadmap - July 2011
- NIST, SP500-292 NIST Cloud Computing reference architecture - Sep. 2011
- NIST, SP500-293 US Government Cloud Computing Technology Roadmap (DRAFT) - Nov. 2011
- NIST, SP500-299 Cloud Computing Security Reference Architecture (DRAFT) - June 2013
- ENISA, Cloud Computing Security Risk Assessment - Nov. 2009
- ENISA, Cloud Computing Information Assurance Framework - Nov. 2009
- Cloud Security Alliance, Cloud Controls Matrix - Sep. 2013
- ISACA, Security Considerations for Cloud Computing - July 2011
- Recommendation ITU-T X.1601, Security framework for cloud computing - Jan. 2014

## Bibliography

- 2 [1] ISO/IEC 17788:201x, Information technology — Distributed application platforms and services  
3 — Cloud computing — Overview and Vocabulary
- 4 [2] ISO/IEC 17789:201x, Information technology — Distributed Application Platforms and Services  
5 — Cloud Computing — Reference Architecture
- 6 [3] ISO/IEC 27001, Information technology – Security techniques – Information security  
7 management systems –Requirements
- 8 [4] ISO/IEC 27005, Information technology – Security techniques – Information security risk  
9 management
- 10 [5] ISO/IEC 27018, Code of practice for PII protection in public clouds acting as PII processors
- 11 [6] ISO/IEC 27036-1, Information technology – Security techniques – Information security for  
12 supplier relationships – Part 1: Overview and concepts
- 13 [7] ISO/IEC FDIS 27036-2, Information technology – Security techniques – Information security for  
14 supplier relationships – Part 2: Requirements
- 15 [8] ISO/IEC 27036-3, Information technology – Security techniques – Information security for  
16 supplier relationships – Part 3: Guidelines for ICT supply chain
- 17 [9] ISO/IEC WD 27036-4, Information technology – Security techniques – Information security for  
18 supplier relationships – Part 4: Guidelines for security of cloud services
- 19 [10] ISO 31000, Risk management – Principles and guidelines
- 20 [11] ITU-T Recommendation X.805 (2003), Security architecture for systems providing end-to-end  
21 communications.
- 22 [12] U.S. CIO Council, Proposed Security Assessment & Authorization for U.S. Government Cloud  
23 Computing
- 24 [13] NIST, SP800-144 Guidelines on Security and Privacy in Public Cloud Computing
- 25 [14] NIST, SP800-145 The NIST Definition of Cloud Computing (Draft)
- 26 [15] NIST, Effectively and Securely Using the Cloud Computing Paradigm
- 27 [16] ENISA, Cloud Computing Benefits, risks and recommendations for information security
- 28 [17] ENISA, Cloud Computing Information Assurance Framework
- 29 [18] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing  
30 V2.1
- 31 [19] Cloud Security Alliance, Top Threats to Cloud Computing V1.0
- 32 [20] Cloud Security Alliance, Domain 12: Guidance for Identity & Access Management V2.1
- 33 [21] Cloud Security Alliance, CSA Cloud Controls Matrix V1.1

- 1 [22] ISACA, Cloud Computing: Business Benefits With Security, Governance and Assurance
- 2 Perspectives
- 3 [23] ISACA, Cloud Computing Management Audit/Assurance Program