

# CCForum Standard

클라우드컴퓨팅표준화포럼(영문표준)

CCF.KO-1055

제정일: 2015년 12월 14일

정보기술 - 보안기술 - 클라우드  
서비스를 위한 ISO/IEC 27002 기반의  
정보보안 통제 실무 지침

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

정보기술 - 보안기술 - 클라우드 서비스를 위한  
ISO/IEC 27002 기반의 정보보안 통제 실무 지침

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



본 문서에 대한 저작권은 클라우드컴퓨팅표준화포럼에 있으며, 클라우드컴퓨팅표준화포럼과 사전 협의 없이 이 문서의 전체 또는 일부를 상업적 목적으로 복제 또는 배포해서는 안 됩니다.

클라우드컴퓨팅표준화포럼표준(영문표준)  
**목 차**

1. 범위.....	1
2. 참조문헌.....	1
3. 용어정의 및 약어.....	1
3.1 용어정의.....	1
3.2 약어.....	2
4. 클라우드 상세영역 개념.....	2
4.1 개요.....	2
4.2 클라우드 서비스에서 공급자 관계.....	3
4.3 클라우드 서비스 소비자 와 클라우드 서비스 제공자 간 관계.....	3
4.4 클라우드 서비스 정보 보안 위기 관리.....	4
4.5 이 표준의 구조.....	4
5. 정보 보안 정책.....	5
5.1 정보 보안을 위한 관리 방향.....	5
6. 정보 보안 구조.....	7
6.1 내부 구조.....	7
6.2 모바일 기기 및 통신판매(텔레마케팅) .....	8
7. 인사 보안.....	9
7.1 고용 전.....	9
7.2 고용 중.....	9
7.3 해지 및 전직.....	10
8. 자산 관리.....	11
8.1 자산에 대한 책임.....	11
8.2 정보 분류.....	11
8.3 매체 취급.....	12
9. 권한 통제.....	13
9.1 권한 통제의 사업 필요조건.....	13
9.2 사용자 권한 관리.....	13
9.3 사용자 책임.....	15
9.4 시스템 및 응용 프로그램 권한 통제.....	15
10. 암호 방식.....	17
10.1 암호 방식 통제.....	17
11. 물리/환경 보안.....	19
11.1 보안 구역.....	19

클라우드컴퓨팅표준화포럼표준(영문표준)

11.2	장비.....	19
12.	운용 보안.....	21
12.1	운용 절차 및 책임.....	21
12.2	악성 코드로부터의 보호.....	22
12.3	백업.....	22
12.4	경과기록(logging) 및 모니터링.....	23
12.5	운용 소프트웨어 규제.....	25
12.6	기술상 취약성 관리.....	25
12.7	정보 시스템 감사 시 고려사항.....	25
13.	통신 보안.....	26
13.1	네트워크 보안 관리.....	26
13.2	정보 전환.....	26
14.	시스템 취득, 개발 및 유지.....	28
14.1	정보 시스템 보안 필요조건.....	28
14.2	개발 중 보안 및 지원 과정.....	28
14.3	테스트 데이터.....	30
15.	공급자 관계.....	31
15.1	공급자 관계의 정보 보안 .....	31
15.2	공급자 서비스 제공 관리.....	32
16.	정보 보안 사건 관리.....	33
16.1	정보 보안 사건 관리 및 개선.....	33
17.	사업 지속성 관리 관련 정보 보안 .....	36
17.1	정보 보안 지속성.....	36
17.2	중복도.....	36
18.	규정 준수.....	37
18.1	법적 및 계약상 필요조건 준수.....	37
18.2	정보 보안 평가.....	38
부속서 A (권고) 클라우드 서비스의 확장된 통제 세트.....		40
CLD.6.3	클라우드 서비스 소비자 및 클라우드 서비스 제공자 간 관계.....	40
CLD.8.1	자산에 대한 책임.....	40
CLD.9.5	공유 가상환경의 클라우드 서비스 소비자 데이터 권한 통제.....	41
CLD.12.1	운용 절차 및 책임.....	42
CLD.12.4	경과기록(logging) 및 모니터링.....	43
CLD.13.1	네트워크 보안 관리.....	44
부속서 B (참고) 클라우드 컴퓨팅 관련 정보 보안 위험 참조.....		45
참고문헌.....		47

## Contents

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 .....	3
	4.3 Relationships between cloud service customers and cloud service providers .....	3
	4.4 Managing information security risks in cloud services .....	4
	4.5 Structure of this standard .....	4
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 .....	11
	8.3 Media handling .....	12
9	Access control .....	13
	9.1 Business requirements of access control .....	13
	9.2 User access management .....	13
	9.3 User responsibilities .....	15
	9.4 System and application access control .....	15
10	Cryptography .....	17
	10.1 Cryptographic controls .....	17
11	Physical and environmental security .....	19
	11.1 Secure areas .....	19
	11.2 Equipment .....	19
12	Operations security .....	21
	12.1 Operational procedures and responsibilities .....	21
	12.2 Protection from malware .....	22

12.3	Backup .....	22
12.4	Logging and monitoring.....	23
12.5	Control of operational software .....	25
12.6	Technical vulnerability management.....	25
12.7	Information systems audit considerations .....	25
13	Communications security.....	26
13.1	Network security management.....	26
13.2	Information transfer .....	26
14	System acquisition, development and maintenance .....	28
14.1	Security requirements of information systems .....	28
14.2	Security in development and support processes .....	28
14.3	Test data .....	30
15	Supplier relationships.....	31
15.1	Information security in supplier relationships .....	31
15.2	Supplier service delivery management .....	32
16	Information security incident management .....	33
16.1	Management of information security incidents and improvements .....	33
17	Information security aspects of business continuity management.....	36
17.1	Information security continuity .....	36
17.2	Redundancies .....	36
18	Compliance .....	37
18.1	Compliance with legal and contractual requirements .....	37
18.2	Information security reviews .....	38
Annex A (normative)	Cloud service extended control set.....	40
CLD.6.3	Relationship between cloud service customer and cloud service provider.....	40
CLD.8.1	Responsibility for assets.....	40
CLD.9.5	Access control of cloud service customer data in shared virtual environment .....	41
CLD.12.1	Operational procedures and responsibilities.....	42
CLD.12.4	Logging and monitoring .....	43
CLD.13.1	Network security management .....	44
Annex B (informative)	References on information security risk related to cloud computing.....	45
Bibliography	.....	47

# 정보기술 – 보안기술 – 클라우드 서비스를 위한 ISO/IEC 27002 기반의 정보보안 통제 실무 지침

## **(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 provision and use 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 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, *Information technology - Security techniques - Information security management systems - Overview and vocabulary*

Recommendation ITU-T Y.3500 | ISO/IEC 17788, *Information technology - Cloud computing — Overview and vocabulary*

Recommendation ITU-T Y.3502 | ISO/IEC 17789, *Information technology - Cloud computing — Reference architecture*

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, Recommendation ITU-T Y.3500 | ISO/IEC 17788, Recommendation ITU-T Y.3502 | ISO/IEC 17789, and the following apply.

##### **3.1.1 capability**

quality of being able to perform a given activity

[SOURCE: ISO 19440:2007, 3.1.5]

##### **3.1.2 data breach**

compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored, or otherwise processed

[SOURCE: ISO/IEC 27040:2014, 3.7]

### 3.1.3

#### **secure multi-tenancy**

type of multi-tenancy that employs security controls to explicitly guard against data breaches and provides validation of these controls for proper governance

Note 1 Secure multi-tenancy exists when the risk profile of an individual tenant is no greater than it would be in a dedicated, single-tenant environment.

Note 2 In very secure environments, even the identity of the tenants is kept secret.

[SOURCE: ISO/IEC 27040:2014, 3.39]

### 3.1.4

#### **virtual machine**

the complete environment that supports the execution of guest software

NOTE A virtual machine is a full encapsulation of the virtual hardware, virtual disks, and the metadata associated with it. Virtual machines allow multiplexing of the underlying physical machine through a software layer called a hypervisor.

[SOURCE: ISO/IEC 17203:2011]

## 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

SLA: Service Level Agreement

VM: Virtual Machine

## 4. Cloud sector-specific concepts

### 4.1 Overview

The use of cloud computing has changed how organizations should assess and mitigate information security risks because of the significant changes in how computing resources are technically designed, operated and governed. Recommendation ITU-T X.1631 | ISO/IEC 27017 provides additional cloud- specific implementation guidance based on ISO/IEC 27002 and provides additional controls to address cloud-specific information security threats and risks considerations.

Users of this Recommendation | International Standard should refer to clauses 5 to 18 in ISO/IEC 27002 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

apply to both the general and cloud computing contexts of the organization. For example, “6.1.2 Segregation of duties” of ISO/IEC 27002 provides a control that can be applied whether the organization is acting as a cloud service provider or not. Additionally, a cloud service customer can derive requirements for segregation of duties in the cloud environment from the same control, e.g., segregating the cloud service customers’ cloud service administrators and cloud service users. 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) that are intended to mitigate the risks that accompany the technical and operational features of cloud services (see Annex B). The cloud service customers and the cloud service providers can refer to ISO/IEC 27002 and this Recommendation | International Standard to select controls with the implementation guidance, and add other controls if necessary. This process can be done by performing an 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 clause 15 “Supplier relationships” provides controls, implementation guidance and other information for managing information security in supplier relationships. The provision and use 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. Therefore, the clause applies to cloud service customers and cloud service providers.

Cloud service customers and cloud service providers 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 cloud service provider is a cloud service customer with respect to the first, and a cloud service provider with respect to the cloud service customer using its service. This example illustrates the case where this Recommendation | International Standard applies to an organization both as a cloud service customer and as a cloud service provider. Because cloud service customers and cloud service providers form a supply chain through the design and implementation of the cloud service(s), clause “15.1.3 Information and communication technology supply chain” of ISO/IEC 27002 applies.

The 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. ISO/IEC 27036 Part 4 deals directly with the security of cloud services in supplier relationships. This standard is also applicable to cloud service customers as acquirers and cloud service providers as suppliers.

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

In the cloud computing environment, cloud service customer data is stored, transmitted and processed by a cloud service. Therefore, a cloud service customer’s business processes can depend upon the information security of the cloud service. Without sufficient control over the cloud service, the cloud service customer might need to take extra precautions with its information security practices.

Before entering into a supplier relationship, the cloud service customer needs to select a cloud service, taking into account the possible gaps between the cloud service customer’s information security requirements and the information security capabilities offered by the service. Once a cloud service is selected, the cloud service customer should manage the use of the cloud service in such a way as to meet its information security requirements. In this relationship, the cloud service provider should provide the information and technical support that are necessary to meet the cloud service customer’s information security requirements. When the information security controls provided by the cloud service provider are pre-set and cannot be changed by the cloud service customer, the cloud service customer might need to implement its own, extra controls to mitigate risks.

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

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

The controls and implementation guidance given in clauses 5 to 18 and Annex A of this Recommendation | International Standard address 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 the applicability of its texts at each clause and paragraph.

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

When an objective with controls, or a control under an objective from ISO/IEC 27002, is needed in addition to those of ISO/IEC 27002, they are given in Annex A: (normative) Cloud service extended control set. When a control of ISO/IEC 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 services**”. The guidance is provided in one of the following two types:

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

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

##### Type 1

Cloud service customer	Cloud service provider

##### Type 2

Cloud service customer	Cloud service provider

Additional information that might need to be considered is provided under the subtitle “**Other information for cloud services**”.

## 5. Information security policies

### 5.1 Management direction for information security

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

#### 5.1.1 Policies for information security

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

#### Implementation guidance for cloud services

Cloud service customer	Cloud service provider
<p>An information security policy for cloud computing should be defined as a topic-specific policy of the cloud service customer. The cloud service customer's information security policy for cloud computing should be consistent with the organization's acceptable levels of information security risks for its information and other assets.</p> <p>When defining the information security policy for cloud computing, the cloud service customer should take the following into account:</p> <ul style="list-style-type: none"> <li>— information stored in the cloud computing environment can be subject to access and management by the cloud service provider;</li> <li>— assets can be maintained in the cloud computing environment, e.g. application programs;</li> <li>— processes can run on a multi-tenant, virtualized cloud service;</li> <li>— the cloud service users and the context in which they use the cloud service;</li> <li>— the cloud service administrators of the cloud service customer who have privileged access;</li> <li>— the geographical locations of the cloud service provider's organization and the countries where the cloud service provider can store the cloud service customer data (even temporarily).</li> </ul>	<p>The cloud service provider should augment its information security policy to address the provision and use of its cloud services taking the following into account:</p> <ul style="list-style-type: none"> <li>— the baseline information security requirements applicable to the design and implementation of the cloud service;</li> <li>— risks from authorized insiders;</li> <li>— multi-tenancy and cloud service customer isolation (including virtualization);</li> <li>— access to cloud service customer assets by staff of the cloud service provider;</li> <li>— access control procedures, e.g. strong authentication for administrative access to cloud services;</li> <li>— communications to cloud service customers during change management;</li> <li>— virtualization security</li> <li>— access to and protection of cloud service customer data;</li> <li>— lifecycle management of cloud service customer accounts;</li> <li>— communication of breaches and information sharing guidelines to aid investigations and forensics</li> </ul>

#### Other information for cloud services

The information security policy for cloud computing of the cloud service customer is one of the topic-specific policies described in ISO/IEC 27002, 5.1.1. The information security policy of an organization deals with its information and business processes. When an organization uses cloud services, it can have a policy for cloud computing as a cloud service customer. An organization's information can be stored and maintained in the cloud computing environment, and the business processes can be operated in the cloud computing

environment. General information security requirements stated in the information security policy at the top level are followed by the policy for cloud computing.

In contrast to this, the information security policy for providing cloud services deals with the cloud service customers' information and business processes, not with the cloud service provider's information and business processes. Information security requirements for the provision of the cloud service should meet those of the prospective cloud service customers. As a result, they might not be consistent with information security requirements of the information and business processes of the cloud service provider. Scope of the policy is often suitably defined in terms of the service, but not solely by organizational structure or physical locations.

Virtualization security in cloud computing has several aspects including lifecycle management of virtual instances, storage and access controls for virtualized images, handling of dormant or offline virtual instances, snapshots, protection of hypervisors and security controls governing use of self-service portals.

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

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

## 6. Organization of information security

### 6.1 Internal organization

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

#### 6.1.1 Information security roles and responsibilities

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

#### Implementation guidance for cloud services

Cloud service customer	Cloud service provider
<p>The cloud service customer should agree with the cloud service provider on an appropriate allocation of information security roles and responsibilities, and confirm that it can fulfil its allocated roles and responsibilities. The information security roles and responsibilities of both parties should be stated in an agreement.</p> <p>The cloud service customer should identify and manage its relationship with the customer support and care function of the cloud service provider.</p>	<p>The cloud service provider should agree and document an appropriate allocation of information security roles and responsibilities with its cloud service customers, its cloud service providers, and its suppliers.</p>

#### Other information for cloud services

Even when responsibilities are determined within and between the parties, the cloud service customer is accountable for the decision to use the service. That decision should be made according to the roles and responsibilities determined within the cloud service customer's organization. The cloud service provider is accountable for the information security stated as part of the cloud service agreement. The information security implementation and provisioning should be made according to the roles and responsibilities determined within the cloud service provider's organization.

Ambiguity in roles and in the definition and allocation of responsibilities related to issues such as data ownership, access control, and infrastructure maintenance, can give rise to business or legal disputes, especially when dealing with third parties.

Data and files on the cloud service provider's systems that are created or modified during the use of the cloud service can be critical to the secure operation, recovery and continuity of the service. The ownership of all assets, and the parties who have responsibilities for operations associated with these assets, such as backup and recovery operations, should be defined and documented. Otherwise, there is a risk that the cloud service provider assumes that the cloud service customer performs these vital tasks (or vice versa), and a loss of data can occur.

#### 6.1.2 Segregation of duties

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

#### 6.1.3 Contact with authorities

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

**Implementation guidance for cloud services**

Cloud service customer	Cloud service provider
The cloud service customer should identify the authorities relevant to the combined operation of the cloud service customer and the cloud service provider.	The cloud service provider should inform the cloud service customer of the geographical locations of the cloud service provider's organization and the countries where the cloud service provider can store the cloud service customer data.

**Other information for cloud services**

Information about geographical locations where the cloud service customer data can be stored, processed or transmitted can help the cloud service customer in determining the supervisory authorities and jurisdictions.

**6.1.4 Contact with special interest groups**

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

**6.1.5 Information security in project management**

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

**6.2 Mobile devices and teleworking**

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

**6.2.1 Mobile device policy**

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

**6.2.2 Teleworking**

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

## **7. Human resource security**

### **7.1 Prior to employment**

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

#### **7.1.1 Screening**

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

#### **7.1.2 Terms and conditions of employment**

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

### **7.2 During employment**

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

#### **7.2.1 Management responsibilities**

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

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

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

**Implementation guidance for cloud services**

Cloud service customer	Cloud service provider
<p>The cloud service customer should add the following items to awareness, education and training programmes for cloud service business managers, cloud service administrators, cloud service integrators and cloud service users, including 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> <li>— applicable legal and regulatory considerations.</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>The cloud service provider should provide awareness, education and training for employees, and request contractors to do the same, concerning the appropriate handling of cloud service customer data and cloud service derived data. This data can contain information confidential to a cloud service customer or be subject to specific limitations, including regulatory restrictions, on access and use by the cloud service provider.</p>

**7.2.3 Disciplinary process**

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

**7.3 Termination and change of employment**

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

**7.3.1 Termination or change of employment responsibilities**

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

## 8. Asset management

### 8.1 Responsibility for assets

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

#### 8.1.1 Inventory of assets

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

#### Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer's inventory of assets should account for information and associated assets stored in the cloud computing environment. The records of the inventory should indicate where the assets are maintained, e.g. identification of the cloud service.	The inventory of assets of the cloud service provider should explicitly identify: <ul style="list-style-type: none"> <li>— cloud service customer data;</li> <li>— cloud service derived data.</li> </ul>

#### Other information for cloud services

There are cloud service applications that provide functions for managing information by adding cloud service derived data to the cloud service customer data. Identifying such cloud service derived data as assets and maintaining them in the inventory of assets can contribute to improving information security.

#### 8.1.2 Ownership of assets

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

#### Other information for cloud services

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 when using a PaaS or IaaS service, whereas for a SaaS service, the application software will belong to the cloud service provider.

#### 8.1.3 The Acceptable use of assets

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

#### 8.1.4 Return of assets

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

### 8.2 Information classification

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

**8.2.1 Classification of information**

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

**8.2.2 Labelling of information**

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

**Implementation guidance for cloud services**

Cloud service customer	Cloud service provider
The cloud service customer should label information and associated assets maintained in the cloud computing environment in accordance with the cloud service customer's adopted procedures for labelling. Where applicable, functionality provided by the cloud service provider that supports labelling can be adopted.	The cloud service provider should document and disclose any service functionality it provides allowing cloud service customers to classify and label their information and associated assets.

**8.2.3 Handling of assets**

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

**8.3 Media handling**

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

**8.3.1 Management of removable media**

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

**8.3.2 Disposal of media**

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

**8.3.3 Physical media transfer**

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

## 9. Access control

### 9.1 Business requirements of access control

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

#### 9.1.1 Access control policy

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

#### 9.1.2 Access to networks and network services

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

#### Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer's access control policy for the use of network services should specify requirements for user access to each separate cloud service that is used.	( 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 deregistration

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.

#### Implementation guidance for cloud services

Cloud service customer	Cloud service provider
( no additional implementation guidance )	To manage access to cloud services by a cloud service customer's cloud service users, the cloud service provider should provide user registration and deregistration functions, and specifications for the use of these functions to the cloud service customer.

### 9.2.2 User access provisioning

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.

**Implementation guidance for cloud services**

Cloud service customer	Cloud service provider
( no additional implementation guidance )	The cloud service provider should provide functions for managing the access rights of the cloud service customer's cloud service users, and specifications for the use of these functions.

**Other information for cloud services**

The cloud service provider should support third party identity and access management technologies for its cloud services and the associated administration interfaces. These technologies can enable easier integration and easier user identity administration between the cloud service customer's systems and the cloud service, and can ease the use of multiple cloud services, supporting such capabilities as single sign-on.

**9.2.3 Management of privileged access rights**

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

**Implementation guidance for cloud services**

Cloud service customer	Cloud service provider
The cloud service customer should use sufficient authentication techniques (e.g. multi-factor authentication) for authenticating the cloud service administrators of the cloud service customer to the administrative capabilities of a cloud service according to the identified risks.	The cloud service provider should provide sufficient authentication techniques for authenticating the cloud service administrators of the cloud service customer to the administrative capabilities of a cloud service, according to the identified risk. For example, the cloud service provider can provide multi-factor authentication capabilities or enable the use of third party multifactor authentication mechanisms.

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

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

**Implementation guidance for cloud services**

Cloud service customer	Cloud service provider
The cloud service customer should verify that the cloud service provider's management procedure for allocating secret authentication information, such as passwords, meets the cloud service customer's requirements.	The cloud service provider should provide information on procedures it provides for the management of the secret authentication information of the cloud service customer, including the procedures for allocating such information and for user authentication.

**Other information for cloud services**

The cloud service customer should control the management of secret authentication information by using its own proprietary or third party identity and access management technologies.

**9.2.5 Review of user access rights**

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

**9.2.6 Removal or adjustment of access rights**

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

**9.3 User responsibilities**

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

**9.3.1 Use of secret authentication information**

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

**9.4 System and application access control**

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

**9.4.1 Information access restriction**

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

**Implementation guidance for cloud services**

Cloud service customer	Cloud service provider
The cloud service customer should ensure that access to information in the cloud service can be restricted in accordance with its access control policy and that such restrictions are realized. 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 its cloud services, its cloud service functions and the cloud service customer data maintained in the service.

**Other information for cloud services**

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

**9.4.2 Secure log-on procedures**

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

**9.4.3 Password management system**

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

**9.4.4 Use of privileged utility programs**

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

**Implementation guidance for cloud services**

Cloud service customer	Cloud service provider
<p>Where the use of utility programs is permitted, the cloud service customer should identify the utility programs to be used in its cloud computing environment, and ensure that they do not interfere with the controls of the cloud service.</p>	<p>The cloud service provider should identify the requirements for any utility programs used within the cloud service.</p> <p>The cloud service provider should ensure that any use of utility programs capable of bypassing normal operating or security procedures is strictly limited to authorized personnel, and that the use of such programs is reviewed and audited regularly.</p>

**9.4.5 Access control to program source code**

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

## 10. Cryptography

### 10.1 Cryptographic controls

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

#### 10.1.1 Policy on the use of cryptographic controls

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

#### Implementation guidance for cloud services

Cloud service customer	Cloud service provider
<p>The cloud service customer should implement cryptographic controls for its use of cloud services if justified by the risk analysis. The controls should be of sufficient strength to mitigate the identified risks, whether those controls are supplied by the cloud service customer or by the cloud service provider.</p> <p>When the cloud service provider offers cryptography, the cloud service customer should review any information supplied by the cloud service provider to confirm whether the cryptographic capabilities:</p> <ul style="list-style-type: none"> <li>meet the cloud service customer's policy requirements;</li> <li>are compatible with any other cryptographic protection used by the cloud service customer;</li> <li>apply to data at rest and in transit to, from and within the cloud service.</li> </ul>	<p>The cloud service provider should provide information to the cloud service customer regarding the circumstances in which it uses cryptography to protect the information it processes. The cloud service provider should also provide information to the cloud service customer about any capabilities it provides that can assist the cloud service customer in applying its own cryptographic protection.</p>

#### Other information for cloud services

In some jurisdictions, it might be required to apply cryptography to protect particular kinds of information, such as health data, resident registration numbers, passport numbers and driver's licence numbers.

#### 10.1.2 Key management

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

**Implementation guidance for cloud services**

Cloud service customer	Cloud service provider
<p>The cloud service customer should identify the cryptographic keys for each cloud service, and implement procedures for key management.</p> <p>Where the cloud service provides key management functionality for use by the cloud service customer, the cloud service customer should request the following information on the procedures used to manage keys related to the cloud service:</p> <ul style="list-style-type: none"> <li>— type of keys;</li> </ul> <p>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;</p> <p>recommended key management procedures for use by the cloud service customer.</p> <p>The cloud service customer should not permit the cloud service provider to store and manage the encryption keys for cryptographic operations when the cloud service customer employs its own key management or a separate and distinct key management service.</p>	<p>( no additional implementation guidance )</p>

## **11. Physical and environmental security**

### **11.1 Secure areas**

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

#### **11.1.1 Physical security perimeter**

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

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

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

#### **11.1.3 Securing offices, rooms and facilities**

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

#### **11.1.4 Protecting against external and environmental threats**

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

#### **11.1.5 Working in secure areas**

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

#### **11.1.6 Delivery and loading areas**

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

### **11.2 Equipment**

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

#### **11.2.1 Equipment siting and protection**

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

#### **11.2.2 Supporting utilities**

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

#### **11.2.3 Cabling security**

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

#### **11.2.4 Equipment maintenance**

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

**11.2.5 Removal of assets**

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

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

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

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

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

**Implementation guidance for cloud services**

Cloud service customer	Cloud service provider
The cloud service customer should request confirmation that the cloud service provider has the policies and procedures for secure disposal or re-use of resources.	The cloud service provider should ensure that arrangements are made for the secure disposal or re-use of resources (e.g. equipment, data storage, files, memory) in a timely manner.

**Other information for cloud services**

Additional information about secure disposal can be found in ISO/IEC 27040

**11.2.8 Unattended user equipment**

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

**11.2.9 Clear desk and clear screen policy**

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

## 12. Operations security

### 12.1 Operational procedures and responsibilities

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

#### 12.1.1 Documented operating procedures

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

#### 12.1.2 Change management

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

#### Implementation guidance for cloud services

Cloud service customer	Cloud service provider
<p>The cloud service customer's change management process should take into account the impact of any changes made by the cloud service provider.</p>	<p>The cloud service provider should provide the cloud service customer with information regarding changes to the cloud service that could adversely affect the cloud service. The following will help the cloud service customer determine the effect the changes can 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 might need to inform the cloud service customer of changes caused by the peer cloud service provider.</p>

#### Other information for cloud services

The list of items that should be included in the notification can be identified in an agreement, e.g. a master service agreement or an SLA.

#### 12.1.3 Capacity management

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

**Implementation guidance for cloud services**

Cloud service customer	Cloud service provider
The cloud service customer should ensure that the agreed capacity provided by the cloud service meets the cloud service customer's requirements.	The cloud service provider should monitor the total resource capacity to prevent information security incidents caused by resource shortages.
The cloud service customer should monitor the use of cloud services, and forecast their capacity needs, to ensure performance of the cloud services over time.	

**Other information for cloud services**

Cloud services involve resources 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. These resources include software, processing hardware, data storage, and network connectivity.

Elastic, scalable and on-demand allocation of resources in a cloud service generally increases the total capacity of the service. However, the cloud service customer should be aware that the resources provided could have capacity constraints. Examples of capacity constraints include the number of processor cores for an application, the amount of storage available, or the network bandwidth available.

The constraints can vary depending on the particular cloud service or the particular subscription that the cloud service customer purchases. If the cloud service customer has requirements that exceed the constraints, the cloud service customer might need to change the cloud service or change the subscription.

In order for the cloud service customer to perform capacity management for cloud services, the cloud service customer should have access to relevant statistics on resource usage, such as:

- statistics for particular time periods;
- maximum levels of resource usage.

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

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

**12.2 Protection from malware**

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

**12.2.1 Controls against malware**

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

**12.3 Backup**

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

**12.3.1 Information backup**

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

**Implementation guidance for cloud services**

Cloud service customer	Cloud service provider
<p>Where the cloud service provider provides backup capability as part of the cloud service, the cloud service customer should request the specifications of the backup capability from the cloud service provider. The cloud service should also verify that they meet their backup requirements.</p> <p>The cloud service customer is responsible for implementing backup capabilities when the cloud service provider provides none.</p>	<p>The cloud service provider should provide the specifications of its backup capabilities to the cloud service customer. The specifications should include the following information, as appropriate:</p> <ul style="list-style-type: none"> <li>— scope and schedule of backups;</li> <li>— backup methods and data formats, including encryption, if relevant;</li> <li>— retention periods for backup data;</li> <li>— procedures for verifying integrity of backup data;</li> <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>

**Other information for cloud services**

The allocation of responsibilities for making backups in the cloud computing environment is often unclear. In the case of IaaS, responsibility for making backups generally resides with the cloud service customer. However, a cloud service customer might not be aware of its responsibility to make backups of all cloud service customer data produced in the cloud computing system, such as executable files produced by the use of development capabilities of a PaaS service.

NOTE Varying levels of backup and restore might be offered as a service at additional cost and, in this case, cloud service customers can choose what and when to backup.

**12.4 Logging and monitoring**

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

**12.4.1 Event logging**

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

**Implementation guidance for cloud services**

Cloud service customer	Cloud service provider
The cloud service customer should define its requirements for event logging and verify that the cloud service meets those requirements.	The cloud service provider should provide logging capabilities to the cloud service customer.

**Other information for cloud services**

The responsibilities of the cloud service customer and the cloud service provider for event logging vary depending on the type of cloud service being used. For example, with IaaS, a cloud service provider's logging responsibility can be limited to that of cloud computing infrastructure components, and the cloud service customer can be responsible for logging the events of its own virtual machines and applications.

**12.4.2 Protection of log information**

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

**12.4.3 Administrator and operator logs**

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

**Implementation guidance for cloud services**

Cloud service customer	Cloud service provider
If a privileged operation is delegated to the cloud service customer, the operation and performance of those operations should be logged. The cloud service customer should determine whether logging capabilities provided by the cloud service provider are appropriate or whether the cloud service customer should implement additional logging capabilities.	( no additional implementation guidance )

**Other information for cloud services**

The allocation of responsibilities between the cloud service customer and the cloud service provider (see 6.1.1) should cover privileged operations related to the cloud service. Monitoring and logging the use of privileged operations are necessary to support preventive and corrective actions against incorrect use of these operations.

**12.4.4 Clock synchronisation**

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

**Implementation guidance for cloud services**

Cloud service customer	Cloud service provider
The cloud service customer should request information about the clock used for the cloud service provider's systems.	The cloud service provider should provide information to the cloud service customer regarding the clock used by the cloud service provider's systems, and information about how the cloud service customer can synchronise local clocks with the cloud service clock.

**Other information for cloud services**

When using cloud services, it is necessary to consider the synchronisation of the cloud service customer's systems with the cloud service provider's systems that are running the cloud services used by the cloud service customer. Without such synchronisation, it can be difficult to reconcile events on the cloud service customer's systems with events on the cloud service provider's systems.

**12.5 Control of operational software**

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

**12.5.1 Installation of software on operational systems**

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

**12.6 Technical vulnerability management**

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

**12.6.1 Management of technical vulnerabilities**

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

**Implementation guidance for cloud services**

Cloud service customer	Cloud service provider
The cloud service customer should request information from the cloud service provider about the management of technical vulnerabilities that can affect the cloud services provided. Cloud service customers should identify which technical vulnerabilities they are responsible for, and clearly define their processes for managing them.	The cloud service provider should make available to the cloud service customer information about the management of technical vulnerabilities that can affect the cloud services provided.

**12.6.2 Restrictions on software installation**

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

**12.7 Information systems audit considerations**

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

**12.7.1 Information systems audit controls**

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

### 13 Communications security

#### 13.1 Network security management

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

##### 13.1.1 Network controls

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

##### 13.1.2 Security of network services

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

##### 13.1.3 Segregation in networks

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

#### Implementation guidance for cloud services

Cloud service customer	Cloud service provider
<p>The cloud service customer should define its requirements for segregating networks to achieve tenant isolation in the shared environment of a cloud service and verify that the cloud service provider meets those requirements.</p>	<p>The cloud service provider should enforce segregation of network access for the following cases:</p> <ul style="list-style-type: none"> <li>— segregation between tenants in a multitenant environment;</li> <li>— segregation between the cloud service provider's internal administration environment and the cloud service customer's cloud computing environment.</li> </ul> <p>Where appropriate, the cloud service provider should help the cloud service customer verify the segregation implemented by the cloud service provider.</p>

#### Other information for cloud services

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.

##### 13.2.1 Information transfer policies and procedures

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

##### 13.2.2 Agreements on information transfer

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

**13.2.3 Electronic messaging**

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

**13.2.4 Confidentiality or non-disclosure agreements**

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

## 14 System acquisition, development and maintenance

### 14.1 Security requirements of information systems

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

#### 14.1.1 Information security requirements analysis and specification

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

##### Implementation guidance for cloud services

Cloud service customer	Cloud service provider
<p>The cloud service customer should determine its information security requirements for the cloud service and then evaluate whether services offered by a cloud service provider can meet these requirements.</p> <p>For this evaluation, the cloud service customer should request information on the information security capabilities from the cloud service provider.</p>	<p>The cloud service provider should provide information to the cloud service customers about the information security capabilities they use. This information should be informative without disclosing information that could be useful to someone with malicious intent.</p>

##### Other information for cloud services

Care should be taken to limit disclosure of implementation details about security controls as they relate to the cloud service being provided to those cloud service customers or potential cloud service customers who have a non-disclosure agreement in place.

#### 14.1.2 Securing applications services on public networks

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

#### 14.1.3 Protecting application services transactions

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

### 14.2 Security in development and support processes

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

#### 14.2.1 Secure development policy

**Implementation guidance for cloud services**

Cloud service customer	Cloud service provider
The cloud service customer should request information from the cloud service provider about the cloud service provider's use of secure development procedures and practices	The cloud service provider should provide information about its use of secure development procedures and practices to the extent compatible with its policy for disclosure.

**Other information for cloud services**

Secure development procedures and practices of the cloud service provider can be critical to SaaS.

**14.2.2 System change control procedures**

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

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

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

**14.2.4 Restrictions on changes to software packages**

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

**14.2.5 Secure system engineering principles**

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

**14.2.6 Secure development environment**

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

**14.2.7 Outsourced development**

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

**14.2.8 System security testing**

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

**14.2.9 System acceptance testing**

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

**Other information for cloud services**

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

### **14.3 Test data**

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

#### **14.3.1 Protection of test data**

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

## 15 Supplier relationships

### 15.1 Information security in supplier relationships

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

#### 15.1.1 Information security policy for supplier relationships

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

##### Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should include the cloud service provider as a type of supplier in its 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 data.	( no additional implementation guidance )

#### 15.1.2 Addressing security within supplier agreements

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

##### Implementation guidance for cloud services

Cloud service customer	Cloud service provider
<p>The cloud service customer should confirm the information security roles and responsibilities relating to the cloud service, as described 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>— technical compliance checking;</li> <li>— security testing;</li> </ul>	<p>The cloud service provider should specify as part of an agreement the relevant information security measures that the cloud service provider will implement to ensure no misunderstanding between the cloud service provider and cloud service customer.</p> <p>The relevant information security measures that the cloud service provider will implement can vary based on the type of cloud service the cloud service customer is using.</p>

<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 the service agreement;</li> <li>— authentication and access control;</li> <li>— identity and access management.</li> </ul>	
--	--

**15.1.3 Information and communication technology supply chain**

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

**Implementation guidance for cloud services**

Cloud service customer	Cloud service provider
( no additional implementation guidance )	<p>If a cloud service provider uses cloud services of peer cloud service providers, the cloud service provider should ensure information security levels to its own cloud service customers are maintained or exceeded.</p> <p>When the cloud service provider provides cloud services based on a supply chain, the cloud service provider should provide information security objectives to suppliers, and request each of the suppliers to perform risk management activities to achieve the objectives.</p>

**15.2 Supplier service delivery management**

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

**15.2.1 Monitoring and review of supplier services**

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

**15.2.2 Managing changes to supplier services**

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

## 16 Information security incident management

### 16.1 Management of information security incidents and improvements

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

#### 16.1.1 Responsibilities and procedures

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

#### Implementation guidance for cloud services

Cloud service customer	Cloud service provider
<p>The cloud service customer should verify the allocation of responsibilities for information security incident management and should ensure that it meets the requirements of the cloud service customer.</p>	<p>As a part of the service specifications, the cloud service provider should define the allocation of information security incident management responsibilities and procedures between the cloud service customer and the cloud service provider.</p> <p>The cloud service provider should provide the cloud service customer with documentation covering:</p> <ul style="list-style-type: none"> <li>— the scope of information security incidents that the cloud service provider will report to the cloud service customer;</li> <li>— the level of disclosure of the detection of information security incidents and the associated responses;</li> <li>— the target time period in which notifications of information security incidents will occur;</li> <li>— the procedure for the notification of information security incidents;</li> <li>— contact information for the handling of issues relating to information security incidents;</li> <li>— any remedies that can apply if certain information security incidents occur.</li> </ul>

#### 16.1.2 Reporting information security events

Control 16.1.2 and the associated implementation guidance and other information specified in ISO/IEC

27002 apply. The following sector-specific guidance also applies.

**Implementation guidance for cloud services**

Cloud service customer	Cloud service provider
<p>The cloud service customer should request information from the cloud service provider about the mechanisms for</p> <ul style="list-style-type: none"> <li>— the cloud service customer to report information security events it has detected to the cloud service provider;</li> <li>— the cloud service provider to report information security events it has detected to the cloud service customer;</li> <li>— the cloud service customer to track the status of a reported information security event.</li> </ul>	<p>The cloud service provider should provide mechanisms for:</p> <ul style="list-style-type: none"> <li>— the cloud service customer to report an information security event to the cloud service provider;</li> <li>— the cloud service provider to report an information security event to a cloud service customer;</li> <li>— the cloud service customer to track the status of a reported information security event</li> </ul>

**Other information for cloud services**

The mechanisms should not only define the procedures but also give essential information like contact phone numbers, emails and service times for both the cloud service customer and the cloud service provider.

An information security event can be detected either by the cloud service customer or by the cloud service provider. Therefore, the main additional responsibility relating to cloud computing is that the party detecting the event should have procedures to report the event to the other party immediately.

**16.1.3 Reporting information security weaknesses**

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

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

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

**16.1.5 Response to information security incidents**

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

**16.1.6 Learning from information security incidents**

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

**16.1.7 Collection of evidence**

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

**Implementation guidance for cloud services**

<b>Cloud service customer</b>	<b>Cloud service provider</b>
The cloud service customer and the cloud service provider should agree upon the procedures to respond to requests for potential digital evidence or other information from within the cloud computing environment	

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

### **17.1 Information security continuity**

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

#### **17.1.1 Planning information security continuity**

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

#### **17.1.2 Implementing information security continuity**

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

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

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

### **17.2 Redundancies**

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

#### **17.2.1 Availability of information processing facilities**

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

## 18 Compliance

### 18.1 Compliance with legal and contractual requirements

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

#### 18.1.1 Identification of applicable legislation and contractual requirements

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

##### Implementation guidance for cloud services

Cloud service customer	Cloud service provider
<p>The cloud service customer should consider the issue that relevant laws and regulations can be those of jurisdictions governing the cloud service provider, in addition to those governing the cloud service customer.</p> <p>The cloud service customer should request evidence of the cloud service provider's compliance with relevant regulations and standards required for the cloud service customer's business. Such evidence can be the certifications produced by third party auditors.</p>	<p>The cloud service provider should inform the cloud service customer of the legal jurisdiction governing the cloud service</p> <p>The cloud service provider should identify its own relevant legal requirements (e.g., regarding encryption to protect PII.) This information should also be provided to the cloud service customer when requested.</p> <p>The cloud service provider should provide the cloud service customer with evidence of its current compliance with applicable legislation and contractual requirements</p>

##### Other information for cloud services

The legal and regulatory requirements that apply to the provision and use of cloud services should be identified, particularly where the processing, storage and communication capabilities are geographically distributed and multiple jurisdictions can be involved.

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

#### 18.1.2 Intellectual property rights

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.

##### Implementation guidance for cloud services

Cloud service customer	Cloud service provider
<p>Installing commercially licensed software in a cloud service can cause a breach of the licence terms for the software. The cloud service customer should have a procedure for identifying cloud-specific licensing requirements before permitting any licensed software to be installed in a cloud service. Particular attention should be paid to cases where the cloud service is elastic and scalable and the software can be run on more systems or processor cores than is permitted by the licence terms</p>	<p>Cloud service provider should establish a process for responding to intellectual property rights complaints.</p>

### 18.1.3 Protection of records

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

#### Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should request information from the cloud service provider about the protection of records gathered and stored by the cloud service provider that are relevant to the use of cloud services by the cloud service customer.	The cloud service provider should provide information to the cloud service customer about the protection of records that are gathered and stored by the cloud service provider relating to the use of cloud services by the cloud service customer.

### 18.1.4 Privacy and protection of personally identifiable information

Control 18.1.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

#### Other information for cloud services

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

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.

#### Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should verify that the set of cryptographic controls that apply to the use of a cloud service comply with relevant agreements, legislation and regulations.	The cloud service provider should provide descriptions of the cryptographic controls implemented by the cloud service provider to the cloud service customer for reviewing compliance with applicable agreements, legislation and regulations.

## 18.2 Information security reviews

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

### 18.2.1 Independent review of information security

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

**Implementation guidance for cloud services**

<b>Cloud service customer</b>	<b>Cloud service provider</b>
<p>The cloud service customer should request documented evidence that the implementation of information security controls and guidelines for the cloud service is in line with any claims made by the cloud service provider. Such evidence could include certifications against relevant standards.</p>	<p>The cloud service provider should provide documented evidence to the cloud service customer to substantiate its claim of implementing information security controls.</p> <p>Where individual cloud service customer audits are impractical or can increase risks to information security, the cloud service provider should provide independent evidence that information security is implemented and operated in accordance with the cloud service provider's policies and procedures. This should be made available to prospective cloud service customers prior to entering a contract. 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. When the independent audit is impractical, the cloud service provider should conduct a self-assessment, and disclose its process and results to the cloud service customer.</p>

**18.2.2 Compliance with security policies and standards**

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

**18.2.3 Technical compliance review**

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

## Annex A (normative) Cloud service extended control set

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.

Any organization intending to implement these controls in an ISMS that is to be conformant to ISO/IEC 27001, extend its SOA (statement of applicability) by including the controls stated in this Annex.

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

Objective: To clarify the relationship regarding shared roles and responsibilities between the cloud service customer and the cloud service provider for information security management.

#### CLD.6.3.1 Shared roles and responsibilities within a cloud computing

##### environment Control

Responsibilities for shared information security roles in the use of the cloud service should be allocated to identified parties, documented, communicated and implemented by both the cloud service customer and the cloud service provider.

##### Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should define or extend its existing policies and procedures in accordance with its use of cloud services, and make cloud service users aware of their roles and responsibilities in the use of the cloud service.	The cloud service provider should document and communicate its information security capabilities, roles, and responsibilities for the use of its cloud service, along with the information security roles and responsibilities for which the cloud service customer would need to implement and manage as part of its use of the cloud service.

##### Other information for cloud services

In cloud computing, roles and responsibilities are typically divided between employees of the cloud service customer and employees of the cloud service provider. The allocation of roles and responsibilities should take account of the cloud service customer data and the cloud service customer applications for which the cloud service provider is a custodian.

### CLD.8.1 Responsibility for assets

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

#### CLD.8.1.5 Removal of cloud service customer assets

##### Control

Assets of the cloud service customer that are on the cloud service provider's premises should be removed, and returned if necessary, in a timely manner upon termination of the cloud service agreement.

**Implementation guidance for cloud services**

Cloud service customer	Cloud service provider
<p>The cloud service customer should request a documented description of the termination of service process that covers return and removal of cloud service customer’s assets followed by the deletion of all copies of those assets from the cloud service provider’s systems.</p> <p>The description should list all the assets and document the schedule for the termination of service, which should occur in a timely manner.</p>	<p>The cloud service provider should provide information about the arrangements for the return and removal of any cloud service customer’s assets upon termination of the agreement for the use of a cloud service.</p> <p>The asset return and removal arrangements should be documented in the agreement and should be performed in a timely manner. The arrangements should specify the assets to be returned and removed.</p>

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

Objective: To mitigate information security risks when using the shared virtual environment of cloud computing.

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

**Control**

A cloud service customer’s virtual environment running on a cloud service should be protected from other cloud service customers and unauthorized persons.

**Implementation guidance for cloud services**

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

**Other information for cloud services**

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

- Network and storage configurations can be virtualized when a software virtualization function provides a virtual environment (e.g. a virtual operating system). In addition, segregation of cloud service customers in software virtualized environments can 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 the “meta-data table” of the cloud service, segregation of information from other cloud service customers can be implemented with 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 apply to the cloud computing environment.

**CLD.9.5.2 Virtual Machine Hardening**

**Control**

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

**Implementation guidance for cloud services**

Cloud service customer	Cloud service provider
When configuring virtual machines, ensure that appropriate aspects are hardened (e.g., only those ports, protocols and services that are needed), and that the appropriate technical measures are in place (e.g. anti-malware, logging) for each virtual machine used.	

**CLD.12.1 Operational procedures and responsibilities**

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

**CLD.12.1.5 Administrator’s operational security**

**Control**

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

**Implementation guidance for cloud services**

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.</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> <p>The document should specify that a supervisor should monitor these operations.</p>	<p>The cloud service provider should provide documentation about the critical operations and procedures to cloud service customers who require it.</p>

**Other information for cloud services:**

Cloud computing has the benefit of rapid provisioning and administration, and on-demand self-service. These operations are 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, mechanisms to safeguard the operations should be considered and, if needed, 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 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 specified aspects of the operation of the cloud services that the cloud service customer uses.

**Implementation guidance for cloud services**

Cloud service customer	Cloud service provider
<p>The cloud service customer should request information from the cloud service provider of the service monitoring capabilities available for each cloud service.</p>	<p>The cloud service provider should provide capabilities that enable the cloud service customer to monitor specified aspects, relevant to the cloud service customer, of the operation of the cloud services. For example, to monitor and detect if the cloud service is being used as a platform to attack others, or if sensitive data is being leaked from the cloud service. Appropriate access controls should secure the use of the monitoring facilities. The facilities should provide access only to information about the cloud service customer's own cloud service instances.</p> <p>The cloud service provider should provide documentation of the service monitoring facilities to the cloud service customer.</p> <p>Monitoring should provide data consistent with the event logs described in clause 12.4.1 and assist with SLA terms.</p>

**CLD.13.1 Network security management**

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

**CLD.13.1.4 Alignment of security management for virtual and physical networks**

**Control**

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

**Implementation guidance for cloud services**

Cloud service customer	Cloud service provider
<p>( no additional implementation guidance )</p>	<p>The cloud service provider should define and document an information security policy for the configuration of the virtual network consistent with the information security policy for the physical network. The cloud service provider should ensure that the virtual network configuration matches the information security policy regardless of the means used to create the configuration.</p>

**Other information for cloud services**

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

NOTE Depending on the type of cloud service, the responsibilities for configuring a virtual network can vary between a cloud service customer and a cloud service provider.

## Annex B (informative)

### References on information security risk related to cloud computing

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 to information security risk assessment and treatment. Following is a list of references that include descriptions of the risk sources and risks in the provision and use 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.

Recommendation ITU-T X.1601, *Security framework for cloud computing* - Jan. 2014

Australian Government Information Management Office, *"Summary of Checkpoints" of Privacy and Cloud Computing for Australian Government Agencies: Better Practice Guide* - Feb. 2013

Australian Cyber Security Centre, *"Cloud Computing Security for Tenants"* - December 2014, [http://www.asd.gov.au/publications/protect/Cloud\\_Computing\\_Security\\_for\\_Tenants.pdf](http://www.asd.gov.au/publications/protect/Cloud_Computing_Security_for_Tenants.pdf)

Australian Cyber Security Centre, *"Cloud Computing Security for Cloud Service Providers"*- December 2014, [http://www.asd.gov.au/publications/protect/Cloud Computing Security for Cloud Service Providers.pdf](http://www.asd.gov.au/publications/protect/Cloud_Computing_Security_for_Cloud_Service_Providers.pdf)

Hong Kong OGCI, *Security & Privacy Checklist for Cloud Service Providers in Handling Personal Identifiable Information in Cloud Platforms* - April 2013

Hong Kong OGCI, *Security Checklists for Cloud Service Consumers* - Jan. 2013

NIST, *SP800-144 Guidelines on Security and Privacy in Public Cloud Computing* - Dec. 2011

NIST, *SP800-146 Cloud Computing Synopsis and Recommendations* - May 2012

SPRING Singapore, *"Annex A: Virtualisation Security Risk Assessment" of Singapore Technical Reference 30:2012 Technical Reference for virtualisation security for servers* - March 2012

SPRING Singapore, *"Annex A: Checklist of security and service level considerations when reviewing SaaS" of Singapore Technical Reference 31:2012 Technical Reference for security and service level guidelines for the usage of public cloud computing services* - March 2012

SPRING Singapore, *"Annex A: Cloud Service Provider Disclosure" of Singapore Standard SS584:2013 Specification for Multi-Tiered Cloud Computing Security* - Aug 2013

SPRING Singapore, *"Annex B: Checklist of security and service level considerations when reviewing IaaS" of Singapore Technical Reference 31:2012 Technical Reference for security and service level guidelines for the usage of public cloud computing services* - March 2012

SPRING Singapore, *Singapore Standard SS584:2013 Specification for Multi-Tiered Cloud Computing Security* - Aug 2013

SPRING Singapore, *Singapore Technical Reference 30:2012 Technical Reference for virtualisation security for servers* - March 2012

SPRING Singapore, *Singapore Technical Reference 31:2012 Technical Reference for security and service*

*level guidelines for the usage of public cloud computing services - March 2012*

US Government FedRAMP PMO, *The FedRAMP Security Controls Baseline Version 2.0 - June 2014*

Cloud Security Alliance, *Cloud Controls Matrix - Sep. 2013*

ENISA, *Cloud Computing Security Risk Assessment - Nov. 2009*

ENISA, *Cloud Computing Information Assurance Framework - Nov. 2009*

ISACA, *Security Considerations for Cloud Computing - July 2011*

**Bibliography**

- [1] ISO/IEC 17203:2011 - *Open Virtualization Format (OVF) specification*
- [2] ISO/IEC 27001, *Information technology - Security techniques - Information security management systems -Requirements*
- [3] ISO/IEC 27005, *Information technology - Security techniques - Information security risk management*
- [4] ISO/IEC 27018, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*
- [5] ISO/IEC 27036-1, *Information technology - Security techniques - Information security for supplier relationships - Part 1: Overview and concepts*
- [6] ISO/IEC 27036-2, *Information technology - Security techniques - Information security for supplier relationships - Part 2: Requirements*
- [7] ISO/IEC 27036-3, *Information technology - Security techniques - Information security for supplier relationships - Part 3: Guidelines for information and communication technology supply chain security*
- [8] ISO/IEC CD 27036-4, *Information technology - Security techniques - Information security for supplier relationships - Part 4: Guidelines for security of cloud services*
- [9] ISO/IEC 27040, *Information technology — Security techniques — Storage security*
- [10] ISO 31000, *Risk management - Principles and guidelines*
- [11] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*
- [12] Recommendation ITU-T X.1601, *Security framework for cloud computing - Jan. 2014*
- [13] NIST, SP800-144 *Guidelines on Security and Privacy in Public Cloud Computing*
- [14] NIST, SP800-145 *The NIST Definition of Cloud Computing*
- [15] NIST, SP800-146 *Cloud Computing Synopsis and Recommendations - May 2012*
- [16] NIST, *Effectively and Securely Using the Cloud Computing Paradigm*
- [17] ENISA, *Cloud Computing Benefits, risks and recommendations for information security*
- [18] ENISA, *Cloud Computing Information Assurance Framework*
- [19] ENISA, *Cloud Computing Security Risk Assessment - Nov. 2009*
- [20] Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing V3.0*
- [21] Cloud Security Alliance, *Top Threats to Cloud Computing V1.0*
- [22] Cloud Security Alliance, *Domain 12: Guidance for Identity & Access Management V2.1*
- [23] Cloud Security Alliance, *CSA Cloud Controls Matrix V3.0*
- [24] ISACA, *Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives*

- [25] ISACA, *Cloud Computing Management Audit/Assurance Program*
- [26] ISACA, *Security Considerations for Cloud Computing - July 2011*

클라우드컴퓨팅표준화포럼표준(영문표준)  
영문 표준 해설서

## 1. 범위

본 표준은 클라우드 서비스 고객(CSC)과 클라우드 서비스 제공자(CSP) 간의 공통된 이해를 기반으로 정보보안 통제를 구현하고 클라우드 서비스의 정보보안 관리에 대한 인증 또는 평가에 필요한 표준화된 기준을 기술한다.

## 2. 참조 문헌

본 표준은 아래의 문헌들을 참조하였다.

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

Recommendation ITU-T Y.3500 | ISO/IEC 17788, *Information technology – Cloud computing – Overview and vocabulary*

Recommendation ITU-T Y.3502 | ISO/IEC 17789, *Information technology – Cloud computing – Reference architecture*

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

## 3. 용어 정의

본 표준은 클라우드 서비스 고객(CSC)과 클라우드 서비스 제공자(CSP) 간의 공통된 이해를 기반으로 정보보안 통제를 구현하고 클라우드 서비스의 정보보안 관리에 대한 인증 또는 평가에 필요한 표준화된 기준과 관련된 용어 및 정의 등을 다룬다.

## 4. 약어

본 표준에는 본 표준에서 사용되는 약어들을 명시한다.

## 5. 규칙

없음

## 6. 표준의 상세 내용

본 표준은 범용 정보보안 통제 실무지침에 대한 국제표준인 ISO/IEC 27002를 기반으로 클라우드 서비스 환경에서 필요한 정보보안 통제를 추가하여 구현 지침을 명시하고 있다. 기존 ISO/IEC 27002의 통제 항목 중에서 35개에 클라우드 서비스 환경의 CSC 또는 CSP를 위한 구현 지침이 추가되었으며, 클라우드 서비스에 특화된 통제항목이 Annex A에 6개 추가된 사항들을 기술한다.

### 부속서 I

클라우드 서비스의 확장된 통제 세트에 관하여 상세히 서술한다.

### 부속서 II

클라우드 컴퓨팅 관련 정보보안 위험 참조에 관하여 상세히 서술한다.

### 참고문헌

본 표준을 작성하는데 사용된 참고 문헌들이 나열되어 있다.

클라우드컴퓨팅표준화포럼표준(영문표준)  
표준 작성 공헌자

표준 번호 : CCF.KO-1055

이 표준의 제.개정 및 발간을 위해 아래와 같이 여러분들이 공헌하셨습니다..

구분	성명	위원회 및 직위	연락처 (E-mail 등)	소속사
표준(과제) 제안	한승한	표준개발분과 간사		한국클라우드산업협회
표준(과제) 작성자	한승한	표준개발분과 간사		한국클라우드산업협회
	전한구	표준개발분과 위원		한국클라우드산업협회
	박대하	표준개발분과 위원		고려사이버대학교
표준 초안 에디터	한승한	표준개발분과 간사		한국클라우드산업협회
	전한구	표준개발분과 위원		한국클라우드산업협회
표준 초안 검토	이강찬	표준개발분과 위원장		한국전자통신연구원
		외 표준개발분과 위원		
표준안 심의	김양우	운영위원회 위원장		동국대학교
		외 운영위원회 위원		
사무국 담당	전한구	-	070-8730-2313 jhg@kcloud.or.kr	한국클라우드산업협회
	한승한	-	070-8730-2389 kinodia@kcloud.or.kr	한국클라우드산업협회

---

클라우드컴퓨팅표준화포럼표준(영문표준)

정보기술 - 보안기술 - 클라우드 서비스를 위한 ISO/IEC 27002 기반의 정보보안  
통제 실무 지침

(Information technology - Security techniques - Code of practice for  
information security controls based on ISO/IEC 27002 for cloud services)

발행인 : 클라우드컴퓨팅표준화포럼 의장

발행처 : 클라우드컴퓨팅표준화포럼

156-827, 서울 동작구 남부순환로 2075 용훈빌딩 6 층

Tel : 070-8730-2389, Fax : 02-2179-8188

발행일 : 2015.12

---