

ISO/IEC JTC 1/SC 27  
IT Security techniques  
Secretariat: DIN (Germany)

**Document type:** Working Draft Text

**Title:** 4thWD 27036-4 20140730

**Status:** As per Resolution 18 (contained in SC 27 N14236 (WG 4 N0443)) of the 16th SC 27/WG 4 meeting, held 2014-04-07 to 2014-04-11 in Hong Kong, China, this document is circulated for review and comment to WG 4 experts, National Bodies and liaison organizations of SC 27/WG 4.

**PLEASE submit your comments on the hereby attached document via the SC 27 e-balloting website at: <http://isotc.iso.org/livelink/livelink/open/jtc1sc27> by the due date 2014-09-30.**

Secretariat's note:

This request for comments will also concurrently be circulated for test purposes ONLY as part of the WG 4 Livelink trial via the Working Group Consultation application accessible at:  
<http://isotc.iso.org/livelink/livelink/open/jtc1sc27wg4>

For the test purposes the WG 4 experts, liaison organizations and National Bodies of SC 27/WG 4 are kindly invited to send their responses to the hereby attached document via the above-mentioned WG 4 Working Group Consultation application.

Any responses received are greatly appreciated and will be taken into account when assessing the trial results and preparing a report to be presented at the October 2014 SC 27 Heads of Delegation meeting in Mexico City, Mexico, 2014-10-23.

**Date of document:** 2014-07-30

**Source:** Project editors

**Expected action:** COMM

**Action due date:** 2014-09-30

**No. of pages:** 1 + 30

**Email of secretary:** [krystyna.passia@din.de](mailto:krystyna.passia@din.de)

**Committee URL:** <http://isotc.iso.org/livelink/livelink/open/jtc1sc27>

# ISO/IEC JTC 1/SC 27 N **14081**

Date: 2014-07-29

**ISO/IEC WD 27036-4.4**

ISO/IEC JTC 1/SC 27/WG 4

Secretariat: DIN

## **Information technology — Security techniques — Information security for supplier relationships — Part 4: Guidelines for security of cloud services**

*Élément introductif — Élément central — Partie 4: Titre de la partie*

### **Warning**

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: International Standard  
Document subtype:  
Document stage: (20) Preparatory  
Document language: E

C:\altes\_NB\Documents\Project\_admin\27036-4\02\_04\_24thWD\_27036-4\_20140730\N14081\_4thWD\_27036-4\_20140730\N14081\_4thWD\_27036-4\_20140730.doc STD Version 2.1c2

### Copyright notice

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

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

Secretariat of ISO/IEC JTC 1/SC 27  
DIN German Institute for Standardization  
DE-10787 Berlin

Tel. + 49 30 2601 2652

Fax + 49 30 2601 1723

E-mail [krystyna.passia@din.de](mailto:krystyna.passia@din.de)

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

<http://isotc.iso.org/isotcportal/index.html> (SC 27 documents)

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

Violators may be prosecuted.

# Contents

Page

Foreword .....	v
Introduction.....	vi
1 Scope .....	1
2 Normative references .....	1
3 Terms and definitions .....	2
4 Structure of this International Standard .....	4
5 Key cloud concepts and security threats and risks .....	5
5.1 Characteristics of cloud computing information security .....	5
5.2 Cloud service threats and associated risks .....	6
5.2.1 Overview.....	6
5.2.2 IaaS and Public Cloud.....	7
5.2.3 PaaS and Public Cloud .....	8
5.2.4 SaaS and Public Cloud .....	8
6 Information security in cloud services (Customer) .....	9
6.1 Agreement processes .....	9
6.1.1 Acquisition process .....	9
6.1.2 Supply process.....	10
6.2 Organisational project-enabling processes .....	10
6.3 Project processes.....	10
6.3.1 Project planning process.....	10
6.3.2 Project assessment and control process .....	10
6.3.3 Decision management process .....	10
6.3.4 Risk management process .....	10
6.3.5 Configuration management process.....	10
6.3.6 Information management process.....	11
6.3.7 Measurement process.....	11
6.4 Technical processes .....	11
6.4.1 Stakeholder requirements definition process .....	11
6.4.2 Requirements analysis process .....	11
6.4.3 Architectural design process .....	11
6.4.4 Implementation process .....	11
6.4.5 Integration process .....	11
6.4.6 Verification process .....	11
6.4.7 Transition process .....	11
6.4.8 Validation process.....	11
6.4.9 Operation process .....	11
6.4.10 Maintenance process .....	12
6.4.11 Disposal process .....	12
7 Information security in cloud services (provider).....	12
7.1 Overview.....	12
7.2 Agreement processes .....	13
7.2.1 Acquisition process .....	13
7.2.2 Supply process.....	13
7.3 Organizational project-enabling processes.....	14
7.4 Project processes.....	14
7.5 Technical processes .....	14
7.5.1 Stakeholder Requirements Definition Process .....	14
7.5.2 Requirements Analysis Process.....	14

7.5.3	Architectural Design Process.....	14
7.5.4	Implementation Process .....	14
7.5.5	Integration Process .....	14
7.5.6	Verification Process .....	14
7.5.7	Transition Process.....	14
7.5.8	Validation Process.....	15
7.5.9	Operation Process .....	15
7.5.10	Maintenance Process .....	15
7.5.11	Disposal Process .....	15
8	Information security controls in cloud services (provider).....	15
8.1	Overview .....	15
8.2	IaaS and Public Cloud .....	16
8.3	PaaS and Public Cloud.....	16
8.4	SaaS and Public Cloud.....	17
8.5	NaaS .....	17
8.6	Hybrid Cloud .....	17
8.7	Private Cloud.....	17
Annex A (informative)	Characteristics of Cloud Services.....	18
Annex B (informative)	<i>Editors note: ISF did not provide material for this annex: we propose to delete it in WD4</i> .....	19
Annex C (informative)	<i>Editors note: change to Annex B, once ISF material deleted</i> Additional security standards that can help cloud services security .....	20
Annex D (informative)	<i>Editors note: change to Annex C, once ISF material deleted</i> Mapping to ISO/IEC 27017 controls .....	23
Bibliography	.....	24

## Foreword

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

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

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

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

ISO/IEC 27036-4 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

ISO/IEC 27036 consists of the following parts, under the general title *Information technology — Security techniques — Information security for supplier relationships*:

*Part 1: Overview and concepts*

*Part 2: Requirements*

*Part 3: Guidelines for ICT supply chain security*

*Part 4: Guidelines for security of cloud services*

## Introduction

This International Standard provides guidance to cloud-based product and service acquirers and suppliers. Its application should result in:

- Increased information security in cloud-based services.
- Increased understanding by the acquirers of the risks associated with cloud services to enhance the implementation of information security requirements.
- Increased ability of cloud service providers to provide assurance to acquirers that they have identified risks in their product(s) or service(s) and associated supply chains and have taken measures to manage those risks.

This International Standard is intended to be used by all types of organizations that acquire or supply cloud-based products and services. The guidance is primarily focused on the initial link of the first acquirer and supplier, but the principal steps should be applied throughout the chain, starting when the first supplier changes its role to being an acquirer and so on. The manner in which this change of roles is repeated and the manner in which the same steps are repeated for each new acquirer-supplier link in the chain is central to this standard. By following the guidance contained within this standard it should be possible to have a seamless linkage of information security priorities visible across the supply chain. Information security concerns related to supplier relationships cover a broad range of scenarios. Organizations that wish to improve trust within their cloud service provision should define their trust boundaries, evaluate the risk associated with their supply chain activities, and then define and implement appropriate risk identification and mitigation techniques to reduce the risk of vulnerabilities being introduced through their cloud service provision supply chain.

ISO/IEC 27001 and ISO/IEC 27002 framework and controls provide a useful starting point for identifying appropriate requirements for acquirers and suppliers. ISO/IEC 27017 and ISO/IEC 27018 provide guidance on how a cloud service provider can implement, manage and operate information security for a cloud service. ISO/IEC 27036 (all parts) provides further detail regarding specific requirements to be used in establishing and monitoring information security in supplier relationships.

Typically, cloud services are purchased 'as is'; an acquirer has little, or no, ability to specify or request changes to the cloud service being purchased. However, in certain cases, the acquirer has the ability to specify the service and the detail of that service, including the information security arrangements required of the supplier. This International Standard is written to cover both of these eventualities. This International Standard is written to cover the first of these eventualities and refers to ISO/IEC 27036 Part 1-3 for the cases when security arrangements can be specified.

*Editor's note: the introduction will be finalised when the detailed content of the standard is agreed.*

# Information technology — Security techniques — Information security for supplier relationships — Part 4: Guidelines for security of cloud services

## 1 Scope

This part of International Standard ISO/IEC 27036 provides acquirers and suppliers of cloud services with guidance on:

- a) gaining visibility into the information security risks associated with the use of cloud services and managing those risks effectively; and
- b) responding to risks specific to the acquisition or provision of cloud-based services that can have an information security impact on organisations using these services.

This part of ISO/IEC 27036 does not include business continuity management/resiliency issues involved with the cloud service. ISO/IEC 27031 addresses business continuity.

This part of ISO/IEC 27036 does not provide guidance on how a cloud service provider should implement, manage and operate information security. Guidance can be found in ISO/IEC 27002 and ISO/IEC 27017. ISO/IEC 27017 states:

The scope of this International Standard is to define guidelines supporting the implementation of Information Security Management for the use of cloud service.

## 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 DIS 17788: Information technology – Cloud computing – Overview and Vocabulary

ISO/IEC DIS 17789: Information technology – Cloud computing – Reference Architecture

ISO/IEC 27017:–<sup>1</sup>, *Information technology – Security techniques – Code of practice for information security controls for cloud computing services based on ISO/IEC 27002*

ISO/IEC 27036-1:–<sup>2</sup>, *Information technology – Security techniques – Information security in supplier relationships – Part 1: Overview and concepts*

ISO/IEC 27036-2:–<sup>3</sup>, *Information technology – Security techniques – Information security in supplier relationships – Part 2: Requirements*

---

<sup>1</sup> To be published.

<sup>2</sup> To be published.



ISO/IEC 27036-3:–<sup>4</sup>, *Information technology – Security techniques – Information security in supplier relationships – Part 3: Guidelines for ICT supply chain security*

### 3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27036-1, ISO/IEC 27036-2 and the following definitions apply.

*Editors Note: Since ISO/IEC 27017 is a Normative Reference, definitions given in ISO/IEC 27017 may not be listed in this clause 3.*

#### 3.1 auditability

property of a process that enables it to be verified for conformance to certain standard

#### 3.2 authenticity

property that an entity is what it claims to be

[SOURCE: ISO/IEC 27000:2013, 2.8]

#### 3.3 cloud computing

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

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

[SOURCE: ISO/IEC 17788]

#### 3.4 cloud service customer

party which is in a business relationship for the purpose of using cloud services (3.6)

NOTE – A business relationship may not necessarily imply financial agreements.

[SOURCE: ISO/IEC 17788 | Y.ccdef]

#### 3.5 cloud service provider

party which makes cloud services (3.6) available

[ISO/IEC 17788 | Y.ccdef]

#### 3.6 cloud service

one or more capabilities offered via cloud computing invoked using a defined interface

[ISO/IEC 17788 | Y.ccdef]

#### 3.7 defence-in-depth

series of protection methods and mechanisms deployed throughout the life cycle

---

<sup>3</sup> To be published.

<sup>4</sup> To be published.

**3.8****Hybrid cloud**

deployment model of cloud computing using at least two different cloud deployment models

*Editors note: the following definition from NIST SP800-145, 2011 is offered for comparison: "The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)."*

**3.9****infrastructure as a service****IaaS**

cloud service category in which the cloud capabilities type provided to the cloud service customer is an infrastructure capabilities type

NOTE – The cloud service customer (3.x) does not manage or control the underlying physical and virtual resources, but may have control over operating systems, storage, and deployed applications that use the physical and virtual resources. The cloud service customer (3.x) may also have limited ability to control certain networking components (e.g., host firewalls).

[ISO/IEC 17788 | Y.ccdef]

**3.10****network as a service****NaaS**

cloud service category in which the capability provided to the cloud service customer is transport, connectivity and related network capabilities

NOTE – NaaS can provide any of the three cloud capabilities types (3.2.3). *Editors note: reference to be checked*

[ISO/IEC 17788 | Y.ccdef]

**3.11****platform as a service****PaaS**

cloud service category in which the cloud capabilities type provided to the cloud service customer (3.4) is a platform capabilities type

[ISO/IEC 17788 | Y.ccdef]

**3.12****private cloud**

cloud deployment model that is used exclusively by a single cloud service customer (3.4) where resources are controlled by that cloud service customer

**3.13****public cloud**

cloud deployment model that is potentially available to any cloud service customer (3.4) where resources are controlled by the cloud service provider

**3.14****software as a service****SaaS**

cloud service category in which the cloud capabilities type provided to the cloud service customer (3.4) is an application capabilities type

[ISO/IEC 17788 | Y.ccdef]

**3.15****system element**

member of a set of elements that constitutes a system

Note 1 to entry: A system element is a discrete part of a system that can be implemented to fulfill specified requirements. A system element can be hardware, software, data, humans, processes (e.g., processes for providing required functionality to users), procedures (e.g., operator instructions), facilities, materials, and naturally occurring entities (e.g., water, organisms, minerals), or any combination.

[SOURCE: ISO/IEC 15288:2008, 4.32]

*{Editors note: propose to delete 3.12, 3.13 and 3.14 (following) as not used in text:}*

### 3.12

#### **Tier 1 supplier**

Direct suppliers of goods, material, services to an acquirer, typically with a business relationship between the supplier and acquirer, defined in a document such as a contract or Service Level Agreement

### 3.13

#### **Tier 2 supplier**

Suppliers of goods, material, services to a Tier 1 supplier – these are indirect suppliers to the Acquirer. Typically, no business relationship exists between the acquirer and the supplier, and a contract and service level agreement typically is not required and not in place

### 3.14

#### **Tier 3 supplier**

Suppliers of goods, material, services to a Tier 2 supplier – these are indirect suppliers to the Acquirer. Typically, no business relationship exists between the acquirer and the supplier, and a contract and service level agreement typically is not required and not in place}

### 3.16

#### **transparency**

property to imply openness and accountability

### 3.17

#### **traceability**

property that allows the tracking of the activity of an identity, process, or an element throughout the supply chain

### 3.18

#### **validation**

confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled

Note 1 to entry: Validation is the set of activities ensuring and gaining confidence that a system is able to accomplish its intended use, goals and objectives (i.e., meet stakeholder requirements) in the intended operational environment.

[SOURCE ISO/IEC 15288:2008, 4.37]

### 3.19

#### **verification**

confirmation, through the provision of objective evidence, that specified requirements have been fulfilled

Note 1 to entry: Verification is a set of activities that compares a system or system element against the required characteristics. This may include, but is not limited to, specified requirements, design description and the system itself.

[SOURCE ISO/IEC 15288:2008, 4.38]

## 4 Structure of this International Standard

This International Standard should be used in combination with the other three parts within ISO/IEC 27036. This fourth part should be used as additional guidelines for information security specifically addressing cloud services.

This International Standard is also harmonized with ISO/IEC 27017 and provides a mapping of ISO/IEC 27017 information security controls to the life cycle processes in Annex D (informative).

*Editors' Note: This clause will be finalized once structures of clauses 5, 6, and 7 are settled.*

## 5 Key cloud concepts and security threats and risks

### 5.1 Characteristics of cloud computing information security

According to the definition of cloud computing, underpinning the cloud services is a number of technologies (such as server virtualisation and Service Oriented Architecture) that enable provision of the service. These cloud services typically use a shared infrastructure which a cloud service provider can move and process a cloud service customer's data to deliver the most efficient service at minimal cost.

The following cloud service categories which are defined in ISO/IEC 17788 are typically shared and consumed by a large number of cloud service consumers in supplier relationship:

- a) Software as a Service (SaaS)
- b) Platform as a Service (PaaS)
- c) Infrastructure as a Service (IaaS)
- d) Network as a Service (NaaS).

These cloud service categories are typically shared and consumed by a large number of cloud service customers in supplier relationship.

To differentiate between the roles in supplier relationships and the specifics regarding cloud services ISO/IEC 27036-4 uses the terms cloud service customer for the acquirer and cloud service provider for the supplier.

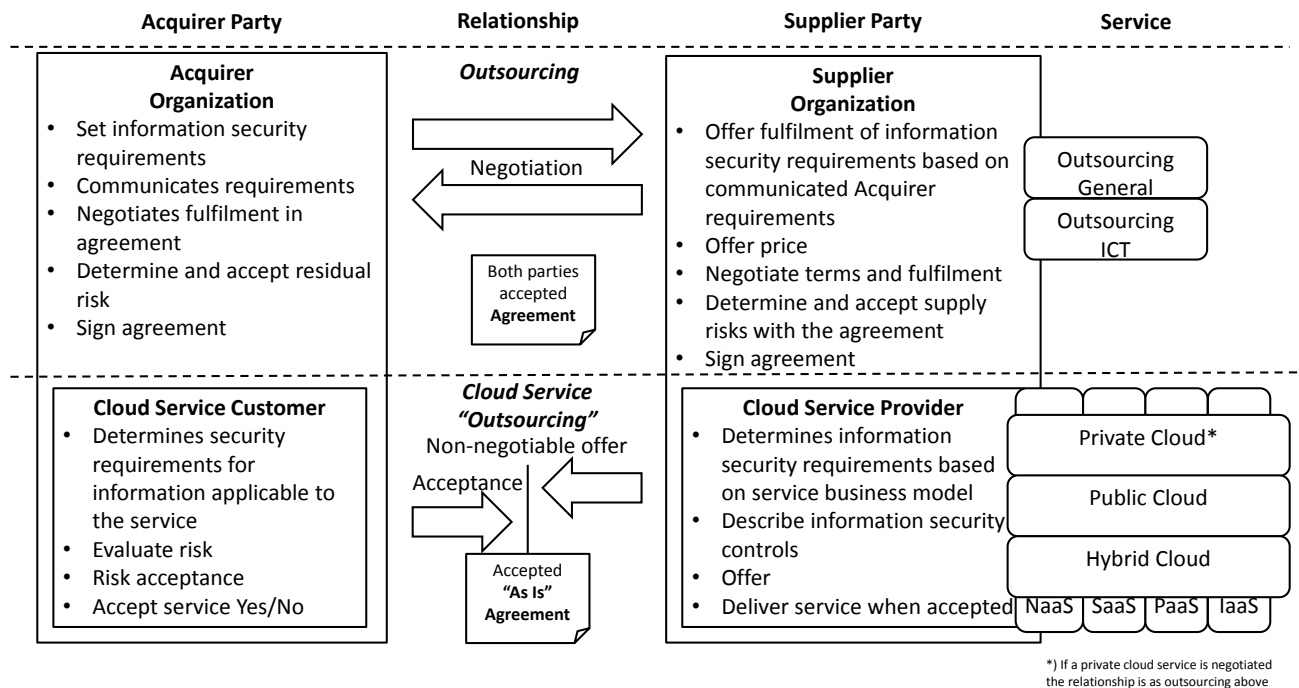
*Editors note: the following paragraph uses expert contributions but has been reworded to improve readability.*

Cloud service customers are responsible and accountable for the information security risk incurred by the use of information system services offered by external suppliers, including cloud service providers. The cloud service customer makes a risk evaluation and decides whether to use the service or not. This decision may also include a choice among different providers of cloud services. As the knowledge of the cloud service customer might be limited the assurance regarding security from the cloud service provider can influence the cloud service customer's decision about using the service. The cloud service provider that offers and explains superior security functionality is more likely to be selected thus reducing the cloud service customer's risks regardless of the customer's risk awareness.

Cloud services differ from other information and outsourcing services as follows:

- a) The cloud service customer may not have the ability to change or otherwise influence the information security requirements provided by the cloud service provider.
- b) The relationship between cloud service customer and provider is focused on the provider communicating their ability to provide both the service and the security to the cloud service consumer, such as providing a list of security controls for the offered services.
- c) The cloud service customer may select the cloud service(s) offered by the cloud service provider and proceeds to use the cloud service without any negotiation or contractual agreement.

Figure 1 summarizes the differences in relationship between a traditional outsourcing and acquisition of cloud services.



*Editors note: order of cloud types in bottom right hand corner of figure revised to match NIST SP800-145, 2011*

*Figure 1: Principle differences in relationship between outsourcing and cloud service "outsourcing"*

## 5.2 Cloud service threats and associated risks

### 5.2.1 Overview

*Editors note: the following expert contribution has been modified for readability*

The risks related to a cloud service differ depending on the combination of cloud service and deployment model. The threats are very similar to those in traditional ICT but the cloud environment does imply changes to the consequences that may accrue to an incident caused by a threat. For example, the "lack of visibility" that a cloud service customer may have into the service provided implies that the customer may have increased difficulty in determining that an incident is in progress and this might delay defensive measures and remediation that would increase the consequence (and therefore the risk). The threat has not changed (eg attack by malware) but the risk has increased due to the increase in consequence due to a delay in incident detection.

It is essential from the cloud service customer perspective that relevant risks are dealt with as part of their risk assessments. The risk evaluation depends on the assets to be transferred and used in the cloud service and significance of those assets to the business.

For the cloud service provider the risk and the threats are linked to the sector where the cloud service and deployment model are applied and to the level of assurance required for cloud service customers, based on the customers' and providers' industry sector regulatory requirements to accept the risks. (For example there are different requirements if the cloud service business is aimed at the health care sector than the building sector).

The difference in risks and threats for cloud service compared to ICT services is influenced by the following factors:

- Lack of transparency
- Lack of visibility

## c) Lack of clear responsibility

*Editors note: we propose to modify the WD3 text to read:*

The three factors listed above may combine to reduce the control cloud service customers have over the location, access, processing and protection of data placed in the cloud. Additionally, cloud service customers may not be made aware of incidents, breaches, failures or other issues affecting the service in a timely manner. The reduced control, coupled with a lack of information about the cloud service performance and security may alter the risks of using the cloud. The cloud service customer will need to evaluate these risks in relation to the data to be placed in the cloud and the dependence of the business on the data and the cloud service.

Cloud Services differ from traditional IT Services in several aspects of information security. The table (Table 1) contrasts key risk areas for traditional in-house IT with Private Cloud and three prevalent public cloud usages models (Infrastructure, Platform, and Software as a Service):

Table 1: Key risk areas for traditional in-house IT and Cloud computing service

	In house IT	Cloud Computing				
		Private Cloud	Public Cloud			
			IaaS	PaaS	SaaS	NaaS*
<b>Physical Security</b>	Customer	Customer	Provider	Provider	Provider	Provider
<b>Security Services</b>	Customer	Customer	Customer	Customer	Provider	Customer or Provider
<b>Workload and Data Protection</b>	Customer	Customer	Customer	Customer	Provider	Customer or Provider
<b>Application Protection</b>	Customer	Customer	Customer	Provider	Provider	Customer or Provider
<b>Supply Chain Protection</b>	Customer	Customer	Customer	Provider	Provider	Customer or Provider

\* Depending on the service provided

*Editors note: NBs are invited to fill in the NaaS column.*

The focus of this clause is the threats and risks related to public cloud services in combination with the deployment models.

Annex TBD provides a list of standards references that contain risks and threats applicable to cloud services.

*Editors note: The TBD Annex is currently under development as a part of ISO/IEC 27017 development. ISO/IEC 27036-4 editors will import the text once it is approved by the ISO/IEC 27017 editing group.*

*Editors note: The following points have been edited for consistency*

### 5.2.2 IaaS and Public Cloud

The typical IaaS threats and risks may include but are not limited to:

- Where is data stored (integrity, privacy and traceability)
- Access availability to stored data (availability)
- How is data communicated (confidentiality, privacy and integrity)

- d) Who has higher privileges (confidentiality, integrity, privacy and traceability)
- e) Malware (such as viruses, Trojans and worms)

### 5.2.3 PaaS and Public Cloud

In addition to typical IaaS threats and risks, the typical PaaS threats and risks may include but are not limited to:

- a) Malware related to unsecure platforms (such as viruses, Trojans and worms)
- b) Access and rights through administrator rights (confidentiality, integrity and privacy)
- c) Lack of log information (integrity and traceability)
- d) Integrity of platforms (availability and integrity)

### 5.2.4 SaaS and Public Cloud

In addition to typical IaaS and PaaS threats and risks, the typical SaaS threats and risks may include but are not limited to:

- a) Malware related to applications (such as viruses, Trojans and worms)
- b) Access and rights through user rights (confidentiality, privacy and integrity)
- c) Lack of log information from application (traceability and integrity)
- d) Uncontrolled application changes (integrity)
- e) Lack of security requirements in application development (confidentiality, integrity, availability, privacy and traceability)

### 5.2.5 NaaS

NaaS has fewer associated threats and risks because the cloud service customer has greater control as the customer manages the resources utilizing the service. The typical NaaS risks and threats may include but are not limited to:

- a) How is data communicated in/between the network/s (confidentiality, privacy and integrity)
- b) Who has higher privileges (Integrity, traceability, confidentiality and privacy)
- c) Malware etc. (all aspects)

### 5.2.6 Hybrid Cloud

Some of the typical risks and threats above may apply depending on the service.

### 5.2.7 Private Cloud

Some of the typical risks and threats above may apply depending on the service. The instantiation of such risks may be adjusted through a dialogue between the parties, with the requirements of the private cloud service customer being tailored as security controls by the provider to mitigate risks to a level acceptable to the customer.

Table 2: Typical threats and risks associated with public cloud

Typical threats and risks	IaaS	PaaS	SaaS
Lack of knowledge where data is stored	X	X	X
Unknown access to stored data	X	X	X
Lack of knowledge about how data is communicated	X	X	X
Unknown superuser, administrator or privileged user access	X	X	X
Lack of protection against malware	X	X	X
Unknown access rights to data		X	X
Lack of log information		X	X
Unknown integrity of platforms		X	X
Uncontrolled application changes			X
Lack of security requirement in application development			X

*Editors note: text in table adopted from US experts and revised*

## 6 Information security in cloud services (Customer)

### 6.1 Agreement processes

#### 6.1.1 Acquisition process

In addition to ISO/IEC 27036-3 cloud service consumers should include the following as a part of the Acquisition Process to ensure they are appropriately managing security risks associated with cloud service acquisition:

- a) Establish a supplier relationship strategy that:
  - 1) provides most appropriate and reliable information about information security by the cloud service provider;
  - 2) assures smooth communication between cloud service consumer and provider
  - 3) defines clear demarcation of roles and responsibilities between cloud service consumer and provider ;
  - 4) Contains measures for mitigating cloud specific risks;
  - 5) Extends existing policy for the use of cloud computing
- b) Establish requirements for handling multi-tenancy and providing logical and physical separation of information for cloud service consumers;
- c) Establish requirements for the secure transfer of cloud service consumer information to other cloud services either as a result of increased demand or during transfer of service from one supplier to another;



- d) Establish requirements for restricting the movement, transmission and storage of information outside of the jurisdiction or jurisdictions agreed by the cloud service consumer and provider;
- e) Define methods and acceptable evidence for assessing cloud service providers regarding ability to provide logical and physical separation of information for cloud service consumers;
- f) Define processes for transition of the product or service to a different cloud service provider upon contract termination including a transition plan.
- g) Define process for deletion of the information which cloud service consumer has in the cloud computing environment and its verification upon contract termination;
- h) Define processes for gathering and analysis of information security specification provided by cloud service provider which includes SLA or other contract documents.

#### **6.1.2 Supply process**

The supply process is addressed in Clause 7.

### **6.2 Organisational project-enabling processes**

For organizational project-enabling processes ISO/IEC 27036-2 and ISO/IEC 27036-3 should be followed.

### **6.3 Project processes**

#### **6.3.1 Project planning process**

Security of cloud services should be considered in this process, but there is no specific guidance in addition to what is provided in ISO/IEC 27036-2 and ISO/IEC 27036-3.

#### **6.3.2 Project assessment and control process**

Security of cloud services should be considered in this process, but there is no specific guidance in addition to what is provided in ISO/IEC 27036-2 and ISO/IEC 27036-3.

#### **6.3.3 Decision management process**

Security of cloud services should be considered in this process, but there is no specific guidance in addition to what is provided in ISO/IEC 27036-2 and ISO/IEC 27036-3.

#### **6.3.4 Risk management process**

In addition to ISO/IEC 27036-3 Acquirers should include the following as a part of the Risk Management Process to ensure they are appropriately managing security risks associated with cloud service acquisition:

- a) Specify the type, classification and importance of information that may be handled in the cloud (e.g. commercial information, intellectual property (IP), legal, regulatory and privileged information, logistical information, management information or personally identifiable information (PII)) should be examined)
- b) Legal / regulatory risks to the organisation (e.g. copyright, data protection, financial regulation, privacy breach and corporate governance).

#### **6.3.5 Configuration management process**

Cloud services security should be considered in this process, but there is no specific guidance in addition to what is provided in ISO/IEC 27036-2 and ISO/IEC 27036-3.

### **6.3.6 Information management process**

Cloud services security should be considered in this process, but there is no specific guidance in addition to what is provided in ISO/IEC 27036-2 and ISO/IEC 27036-3.

### **6.3.7 Measurement process**

Cloud services security should be considered in this process, but there is no specific guidance in addition to what is provided in ISO/IEC 27036-2 and ISO/IEC 27036-3.

## **6.4 Technical processes**

### **6.4.1 Stakeholder requirements definition process**

Cloud services security should be considered in this process, but there is no specific guidance in addition to what is provided in ISO/IEC 27036-2 and ISO/IEC 27036-3.

### **6.4.2 Requirements analysis process**

For Requirements analysis process there are no cloud specific guidance

### **6.4.3 Architectural design process**

The customer should define processes for transition of the product or service to a different cloud service provider upon contract termination including a transition plan.

### **6.4.4 Implementation process**

When cloud service customer treats sensitive or critical information on a cloud computing service, the cloud service customer should deploy the service by a phased approach in order to reduce risks; cloud service customer should deploy a part of service which has smaller risks, and expand its use while over-viewing the situation.

### **6.4.5 Integration process**

For integration process there are no cloud specific guidance

### **6.4.6 Verification process**

For verification process there are no cloud specific guidance.

### **6.4.7 Transition process**

For transition design process there are no cloud specific guidance

### **6.4.8 Validation process**

For validation design process there are no cloud specific guidance

### **6.4.9 Operation process**

The following requirements should be also considered by the cloud service customer:

- a) Define a “cloud use policy” and arrange training for personnel.
- b) Determine any system limitations that may impact operational information security processes once the services go live.

In addition to ISO/IEC 27036-3 cloud service customers should include the following as a part of the Operation process to ensure they are appropriately managing security risks associated with cloud service acquisition:

- a) Obtain information such as critical system changes and address the changes.
- b) Collect information on and respond to the information security incidents.

#### **6.4.10 Maintenance process**

For maintenance process there is no cloud specific guidance.

#### **6.4.11 Disposal process**

In addition to ISO/IEC 27036-3 cloud service customers should include the following as a part of the Operation process to ensure they are appropriately managing security risks associated with cloud service acquisition:

- a) Confirmation of information disposal at termination of service use.

### **7 Information security in cloud services (provider)**

#### **7.1 Overview**

*Editors note: the following text has been changed to improve readability*

A cloud service provider can provide increased trust to potential and existing cloud service customers by providing information security on two viewpoints:

- a) The cloud service provider as an organisation aligns the part of the organisation providing the actual cloud service(s) with ISO/IEC 27001 ISMS requirements.
- b) The actual service provided is aligned with a number of security controls, depending on the nature of the service and the market and requirements the service is intended for.

The business model driving the cloud service provider should state that certain information security requirements of the cloud service customer(s) are met. This should be communicated to the possible cloud service customer of the cloud service by referring to the standards and requirements the cloud service fulfils and what responsibility the cloud service provider has. However, the cloud service customer should accept the cloud service and its risks.

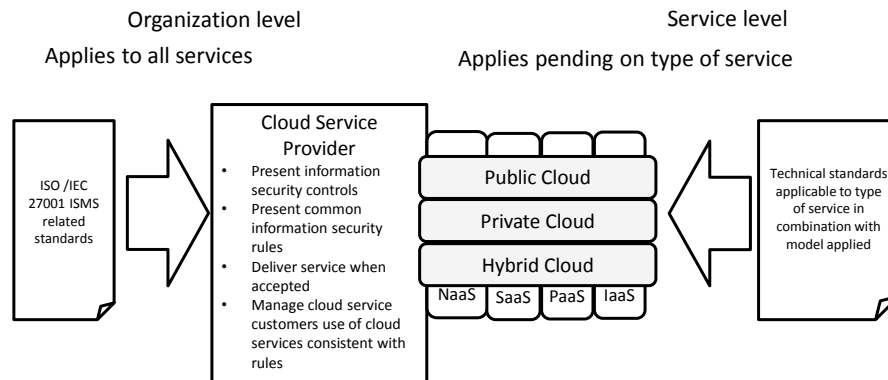


Figure 2. Extended principle use of security standards for a supplier of "Cloud" services

For further mapping of relevant controls to cloud services and deployment models see App XX

*Editors Note: Editors request for NBs to submit contributions on the above figure 3.*

## 7.2 Agreement processes

### 7.2.1 Acquisition process

The Acquisition process is addressed in Clause 6.

### 7.2.2 Supply process

In addition to ISO/IEC 27036-3 cloud service providers should include the following as a part of the Acquisition Process to ensure they are appropriately addressing security risks associated with cloud service acquisition:

- a) The scope of responsibility which cloud service provider should accept. When the cloud service provider is a consumer of other cloud services, the cloud service provider should also specify the responsibility for the use;
- b) The scope of responsibility which cloud service customer should accept;
- c) Information and functionality which cloud service provider should provide for provisioning information security of cloud service consumer including:
  - a) category;
  - b) content;
  - c) time for provision;
  - d) mechanism for provision;
  - e) terms and conditions of providing such as special contract, cost, and so on;

If possible, cloud service provider should also include in the above that cloud service provider is able to disclose an audit report which assures the reliability of the information provided and the certainty of the information security controls of the cloud service provider.

- d) Methods for providing audit, assessment or reviews of the product or service to the cloud service consumer;
- e) Evidence of secure back-up/archive capability;
- f) Evidence of resilience measures (including business continuity and disaster recovery plans) for the provided cloud-based services
- g) A process to notify cloud service customer where more than one cloud service provider is involved in providing the service;
- h) A process for notifying cloud service consumers of changes in cloud suppliers;
- i) Provision of assurance evidence such as third party audit certificates (or) audit / attestation reports, etc.

### **7.3 Organizational project-enabling processes**

For organizational project-enabling processes there is no cloud specific guidance.

### **7.4 Project processes**

For project process there is no cloud specific guidance.

### **7.5 Technical processes**

#### **7.5.1 Stakeholder Requirements Definition Process**

For stakeholder requirements definition process there is no cloud specific guidance.

#### **7.5.2 Requirements Analysis Process**

For requirements analysis process there is no cloud specific guidance.

#### **7.5.3 Architectural Design Process**

For architectural design process there is no cloud specific guidance.

#### **7.5.4 Implementation Process**

For implementation process there is no cloud specific guidances.

#### **7.5.5 Integration Process**

For integration process there is no cloud specific guidance.

#### **7.5.6 Verification Process**

For verification process there is no cloud specific guidance.

#### **7.5.7 Transition Process**

For transition process there is no cloud specific guidance.

### 7.5.8 Validation Process

For validation process there is no cloud specific guidance.

### 7.5.9 Operation Process

In addition to ISO/IEC 27036-3, suppliers should include the following as a part of the operation process to ensure they are appropriately addressing security risks associated with cloud service acquisition:

- a) Cloud service provider should provide information and functionality that is defined in supply process to cloud service consumer.
  - i. Establish an operation process to provide the information and functionality appropriately to cloud service consumer;
  - ii. Provide information and functionality through the operation process;
  - iii. Monitor to ensure that the process is operated appropriately and to audit the process when necessary.
- b) Cloud service provider should monitor the behaviour of cloud service customers and manage them so that cloud service customers observe common information security rules.

### 7.5.10 Maintenance Process

For maintenance process there are no cloud specific guides.

### 7.5.11 Disposal Process

In addition to ISO/IEC 27036-3, suppliers should include the following as a part of the disposal Process to ensure they are appropriately addressing security risks associated with cloud service acquisition:

- a) When a cloud service provider sanitizes information belonging to a cloud service consumer when the consumer terminates use of the cloud service, the provider should produce proof of sanitization for that customer's information;
- b) Cloud service providers should establish a procedure allowing a cloud service customer to request copies of the proof of sanitization.

## 8 Information security controls in cloud services (provider)

*EDITORS NOTE: The NBs should keep in mind that cloud service provider should anticipate their cloud security needs based on the industry context (sector), geography, legal context, etc. The NBs should also keep in mind that the need to comply with legal and regulatory requirements is with the customer.*

### 8.1 Overview

The controls applied to mitigate risks and threats related to a cloud service may differ depending on the combination of service, model, and target customer profile.

Depending on the cloud service customer risk appetite that the cloud service provider sees as the user of the actual cloud service, controls should be applied to meet the acceptance criteria.

*Editors note: we propose to change this sentence to: Controls should be applied by the cloud service provider to meet the risk appetite and the requirements of the cloud service customer*

A cloud service provider that wants to attract cloud service customers with high demands on security has to apply more protection and provide a higher degree of assurance to the market. This means that the cloud service provider should anticipate the cloud customer's cloud security needs based on the industry context (sector), geography, legal context, etc. The cloud service provider should also keep in mind that the need to comply with legal and regulatory requirements is with the consumer but the ability to address this with the cloud service is part of the business success of the provider of the actual cloud service.

It is likely that the cloud service customer has already a set of requirements that has to be met and by using standards and referring to them the cloud service provider can more easily demonstrate how the requirements can be met and then gain acceptance from the cloud service customer.

Any Cloud Service Provider should consider, in general, having:

- a) an ISMS in place (ISO/IEC 27001);
- b) the required control set for the organization;
- c) the required control set for the actual cloud service;
- d) a policy, statement or other communication method to state the information security of the service to actual and potential cloud service customers.

Having an ISMS should be the basic platform for information security within the organization of the cloud service provider.

The actual control set should then vary depending on the cloud service in combination with deployment model and the anticipated acceptance criteria by the cloud service customer. In what way the controls are implemented should also be of concern, which should be determined by the Cloud Service Provider and communicated to the market/intended consumers. Note that lack of controls etc. for the actual cloud service will result in less implemented information security and that can be an active choice by the Cloud Service Provider for business reasons.

The focus of this clause is the control set related to public cloud deployment model in combination with different cloud services. The area of controls is addressed in this clause as the basis for control sets and specific and detailed controls as are to be found in other standards.

NOTE: For reference to other standards see Annex C.

### 8.2 IaaS and Public Cloud

IaaS controls are related to:

- a) Network security (including network access);
- b) Communication security (including cryptography);
- c) Storage security (including physical storage and security during the lifecycle);
- d) Malware protection;
- e) Monitoring;
- f) Capacity;

### 8.3 PaaS and Public Cloud

IaaS controls apply but further PaaS controls increase in the terms of:

- a) Access (user and administrative);
- b) Logging;
- c) OS Integrity;
- d) OS change.

#### **8.4 SaaS and Public Cloud**

IaaS and PaaS controls apply but further SaaS controls increase in the terms of:

- a) Access and user rights;
- b) Application changes;
- c) Application services usage and transfer;
- d) Application development.

#### **8.5 NaaS**

NaaS has in general less need of controls as the Cloud Service Consumer party manages the resources utilizing the service. Basic set of controls are related to:

- a) Responsibility between the parties;
- e) Network security;
- f) Communication security;
- g) Anti virus and malware.

#### **8.6 Hybrid Cloud**

All controls above may apply depending on the service.

#### **8.7 Private Cloud**

All controls above may apply but depend on the service. These controls can be adjusted in dialogue between the parties by requirements of the private cloud service customer and the security controls tailor made, depending on the business case for each service provided.



## Annex A (informative)

### Characteristics of Cloud Services

*Editors Note: Editors soliciting expert contributions to extend this table to cover the different service and deployment model, i.e. expand to be a matrix combining NaaS, SaaS, PaaS, IaaS with Public Cloud, Private Cloud, Hybrid Cloud and what differences there are as described in current table.*

Type of cloud service	Criteria	Cloud Service criteria characteristics	ICT outsourcing criteria characteristics	Notes
NaaS				
SaaS	Service	Generic	Negotiable	
	Infrastructure	Single and shared	Dedicated	
	Tailoring	No	Yes	
	Charging	Measured and fixed fee	Negotiable	
	Auditing or assessment	No	Yes	
	Info. Sec. requirements	Fixed	Negotiable	
PaaS	Service	Generic	Negotiable	
	Infrastructure	Shared	Dedicated	
	Tailoring	No	Yes	
	Charging	Measured and fixed fee	Negotiable	
	Auditing or assessment	No	Yes	
	Info. Sec. requirements	Fixed	Negotiable	
IaaS	Service	Generic	Negotiable	
	Infrastructure	Shared	Dedicated	
	Tailoring	No	Yes	
	Charging	Measured and fixed fee	Negotiable	
	Auditing or assessment	No	Yes	
	Info. Sec. requirements	Fixed	Negotiable	

## Annex B (informative)

*Editors note: ISF did not provide material for this annex: we propose to delete it in WD4*

27036-2 key processes	Sub-process	SCIRAP Step
Agreement processes	<ul style="list-style-type: none"> <li>Acquisition process</li> <li>Supply process</li> </ul>	
Organisational project-enabling processes	<ul style="list-style-type: none"> <li>Life cycle model management process</li> <li>Infrastructure management process</li> <li>Project portfolio management process</li> <li>Human resource management process</li> </ul>	
Project processes	<ul style="list-style-type: none"> <li>Project planning process</li> <li>Project assessment and control process</li> <li>Decision management process</li> <li>Risk management process</li> <li>Configuration management process</li> <li>Information management process</li> <li>Measurement process</li> </ul>	
Technical processes	<ul style="list-style-type: none"> <li>Architectural design process</li> </ul>	
Information security in a supplier relationship instance	<ul style="list-style-type: none"> <li>Supplier relationship planning process</li> <li>Supplier selection process</li> <li>Supplier relationship agreement process</li> <li>Supplier relationship management process</li> <li>Supplier relationship termination process</li> </ul>	<ul style="list-style-type: none"> <li>TBD</li> <li>D.7.2</li> <li>D.7.5</li> <li>D.7.6</li> <li>D.7.7.</li> </ul>

## Annex C (informative)

*Editors note: change to Annex B, once ISF material deleted*

### Additional security standards that can help cloud services security

*Editors Note: Editors are looking for contributions towards an informative annex that could list the standards security measures and controls that can be found in other ISO standards that are applicable to cloud services security.*

*This could be the placeholder during work with 27036-4 for development work. But at the end it should serve as one piece of information where a Cloud Service Provider to find guidance of what controls should be applied to provide assurance to the Cloud Service Consumer. And by that support in more detail the guidance text provided in the main body of the standard.*

*Note: This annex shall not be detailed and repeating other standards but make clear overview and reference to a control.*

*For example Naas: 27033 xx-yy, 27002 10.x,  
27018. Z etc.*

*EDITORS NOTE: Comment IN-15 from HK deferred to MX: The standard can provide reference to the "Cloud Security Alliance checklist". Resolution reads: Deferred until 27017 has a checklist in Annex C.*

*EDITORS NOTE: the editors welcome NB inputs to complete this table.*

Cloud Service	Model	Information Security subject (Clause 7)	ISO/IEC 27002 Control	ISO/IEC 27017 Control	ISO/IEC supporting standard	Privacy ISO/IEC 27018
IaaS	Public Cloud	Network security (including network access)	9.2.3, 9.2.5, 9.2.6, 12.6.1, 13.1.1, 13.1.2, 13.1.3,	tbd	27033, 27032	(Yes)
IaaS	Public Cloud	Communication security (including cryptography)	10.1.1, 10.1.2, 13.1.2, 13.2.3, 18.1.5		27033, (WG2?)	(Yes)
IaaS	Public Cloud	Storage security (including physical storage and security during the lifecycle)	8.1.1, 8.1.2, 8.1.3,		27040, 27031	Yes

			8.3.2, 11.2.7, 17.2			
IaaS	Public Cloud	Anti virus and malware	12.2.1			No
IaaS	Public Cloud	Monitoring	12.4.3, 12.4.4		27033	No
IaaS	Public Cloud	Capacity	12.1.3			No
PaaS	Public Cloud	All	Controls above applies	Controls above applies	Ref above applies	As below
PaaS	Public Cloud	Access (user and adm)	9.2.1, 9.2.2, 9.2.4, 9.3.1, 9.4.2, 9.4.3, 9.4.5			(Yes)
PaaS	Public Cloud	Logging	12.4.1, 12.4.2			(Yes)
PaaS	Public Cloud	OS Integrity	12.6.1			No
PaaS	Public Cloud	OS change	12.1.1, 12.1.2, 12.5.1, 14.2.2			No
SaaS	Public Cloud	All	Controls above applies	Controls above applies	Ref above applies	As below
SaaS	Public Cloud	Access and user rights	9.4.1, 9.4.4		27032	Yes
SaaS	Public Cloud	Application changes	12.6.2		27032	Yes
SaaS	Public Cloud	Application services usage and transfer	14.1.2,		27032	Yes

			14.1.3,			
SaaS	Public Cloud	Application development	14.2.1, 14.2.4, 14.2.5, 14.2.6, 14.2.8, 14.2.9 14.3.1		27032	Yes

## **Annex D** (informative)

*Editors note: change to Annex C, once ISF material deleted*

### **Mapping to ISO/IEC 27017 controls**

*Editors' Note: NBs are invited to submit contributions to this Annex.*

<b>ISO/IEC 27036-4 Clause/Subclause</b>	<b>ISO/IEC 27017 Clause/Subclause</b>

## Bibliography

- [1] ISO/IEC 27018:–<sup>5</sup>, Information technology – Security techniques – Code of practice for data protection controls for public cloud computing services

---

<sup>5</sup> To be published.