

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

Document type: Working Draft Text

Title: WG4N0385_Text_3rdWD_27036-4_20140113

Status: As per resolution 20 (contained in SC 27 N13271) of the 15th SC 27/WG 4 plenary meeting, held 2013-10-21 to 2013-10-25, Incheon, Korea, 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 2014-03-15.

Secretariat's note:

This request for comments is also concurrently being circulated as WG 4 document N0385 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 National Bodies and liaison organizations 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 April 2014 SC 27 Plenary in Hong Kong, 2014-04-14/15.

Date of document: 2014-01-17

Source: Project editors

Expected action: COMM

Action due date: 2014-03-15

No. of pages: 1 + 1 + 21

Email of secretary: krystyna.passia@din.de

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

ISO/IEC JTC 1/SC 27/WG 4
Security controls and services
Convenorship: SABS (South Africa)

Replaces: N 246

Document type: Request for comments

Title: Text 3rdWD 27036-4 - Text for ISO/IEC 3rd WD 27036-4, Information technology – Security techniques – Information security for supplier relationships – Part 4: Guidelines for security of cloud services

Status: As per resolution 20 (contained in SC 27 N13271) of the 15th SC 27/WG 4 plenary meeting, held 2013-10-21 to 2013-10-25, Incheon, Korea, this document is circulated for review and comment to WG 4 experts, National Bodies and liaison organizations of SC 27/WG 4.

A Working group consultation will be created for submissions to this request. Submissions should be sent directly via the SC 27/WG 4 commenting website at

<http://isotc.iso.org/livelink/livelink/open/jtc1sc27wg4> before the action due date.

A request for review and comment will be issued in parallel by SC 27 as SC 27 N13300.

Date of document: 2014-01-13

Source: Editor

Expected action: ACT

Action due date: 2014-03-15

No. of pages: 1 + 21

Email of secretary:

Committee URL: <http://isotc.iso.org/livelink/livelink/open/jtc1sc27wg4>

ISO/IEC JTC 1/SC 27 N **13300**

Date: 2013-12-22

ISO/IEC WD 27036-4.3

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

D:\ISO\isomacroserver-
prod\temp\DOCX2PDFISOTC\DOCX2PDFISOTC.SYSTEM@SRVWEB100_568\16398672_1.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

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	iv
Introduction.....	v
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
6 Information security in cloud services (Consumer)	6
6.1 Agreement processes	6
6.1.1 Acquisition process	6
6.1.2 Supply process.....	7
6.2 Organisational project-enabling processes	7
6.3 Project processes.....	7
6.3.1 Project planning process.....	7
6.3.2 Project assessment and control process	7
6.3.3 Decision management process	7
6.3.4 Risk management process.....	7
6.3.5 Configuration management process.....	8
6.3.6 Information management process.....	8
6.3.7 Measurement process.....	8
6.4 Technical processes	8
7 Information security controls in cloud services (provider)	8
7.1 Overview.....	8
7.2 Agreement processes	9
7.2.1 Supply process.....	9
Annex A (informative) Characteristics of Cloud Services	11
Annex B (informative) xxxx	12
Annex C (informative) Additional security standards that can help cloud services security	13
Annex D (informative) Mapping to ISO/IEC 27017 controls	14
Bibliography.....	15

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. This change of roles and applying the same steps for each new acquirer-supplier link in the chain is the essential intention of the standard. By following this international standard it should enable the transfer of information security implications that determines the visibility of information security risks and the transparency throughout the chain.

Information security concerns related to supplier relationships cover a broad range of scenarios. Organizations desiring 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 cloud service acquirers and suppliers 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 27017:—¹, *Information technology – Security techniques – Code of practice for information security controls for cloud computing services based on ISO/IEC 27002*

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

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

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

¹ To be published.

² To be published.

³ To be published.

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

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

[SOURCE: ISO/IEC 27017–⁵, 3.1.4]

3.4 cloud consumer

person or organization that has a relationship with and uses services from cloud providers (3.5)

[SOURCE: ISO/IEC 27017–⁶, 3.1.7]

3.5 cloud provider cloud service provider

person, organization or entity responsible for making a service available to cloud consumer (3.4)

[SOURCE: ISO/IEC 27017–⁷, 3.1.8]

3.6 cloud service

function useful to a cloud consumer (3.5) provided by a cloud provider (3.6)

[SOURCE: ISO/IEC 27017–⁸, 3.1.5]

3.7 defence-in-depth

series of protection methods and mechanisms deployed throughout the life cycle

⁴ To be published.

⁵ To be published.

⁶ To be published.

⁷ To be published.

⁸ To be published.

3.8**infrastructure as a service****IaaS**

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

Note 1 to entry: The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

[SOURCE: ISO/IEC 27017—⁹, 3.1.10]

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

capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider

Note 1 to entry: The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

[SOURCE: ISO/IEC 27017—¹⁰, 3.1.12]

3.15**software as a service****SaaS**

capability provided to the consumer to use the provider's applications running on a cloud infrastructure

Note 1 to entry: The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

[SOURCE: ISO/IEC 27017—¹¹, 3.1.15]

3.16**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]

3.17**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

⁹ To be published.

¹⁰ To be published.

¹¹ To be published.

3.18

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

3.19

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

3.20

transparency

property to imply openness and accountability

3.21

traceability

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

[SOURCE:]

3.22

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]

3.23

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

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable resources (e.g. networks, servers and storage systems), applications and services that can be rapidly provisioned and released with minimal management effort or service provider interaction. [ISO/IEC 27017] Underpinning the cloud services is a number of technologies (such as server virtualisation and Service Oriented Architecture) that enable provision of the service. These services typically use a shared infrastructure around which a service provider can move a cloud consumer's information and processing to deliver the most efficient service at minimal cost.

ISO/IEC 17788 defines the following service categories for cloud service:

- 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 acquirers 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 Consumer for acquirer and Cloud Service provider for supplier.

The cloud consumer makes a risk evaluation and decides whether to use the service. This decision may also include a choice between different providers of the needed cloud service. As the knowledge of the consumer might be limited the assurance regarding security from the cloud service provider can influence the decision. The Cloud Provider offering and explaining the best security functionality have an advantage and are more likely to be selected.

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

- a) Acquirers do not have the ability to change or otherwise influence the information security requirements provided by the cloud service.
- b) Relationship between Acquirer and Supplier is focused on supplier communicating their ability to provide security to the Acquirer
- c) No negotiation takes place and Acquirer makes the decision to use the service based on what is offered
- d) The Acquirer decision should be risk-based.

Figure 2 provides a summary of the difference in relationship between a traditional outsourcing and acquisition of cloud services.

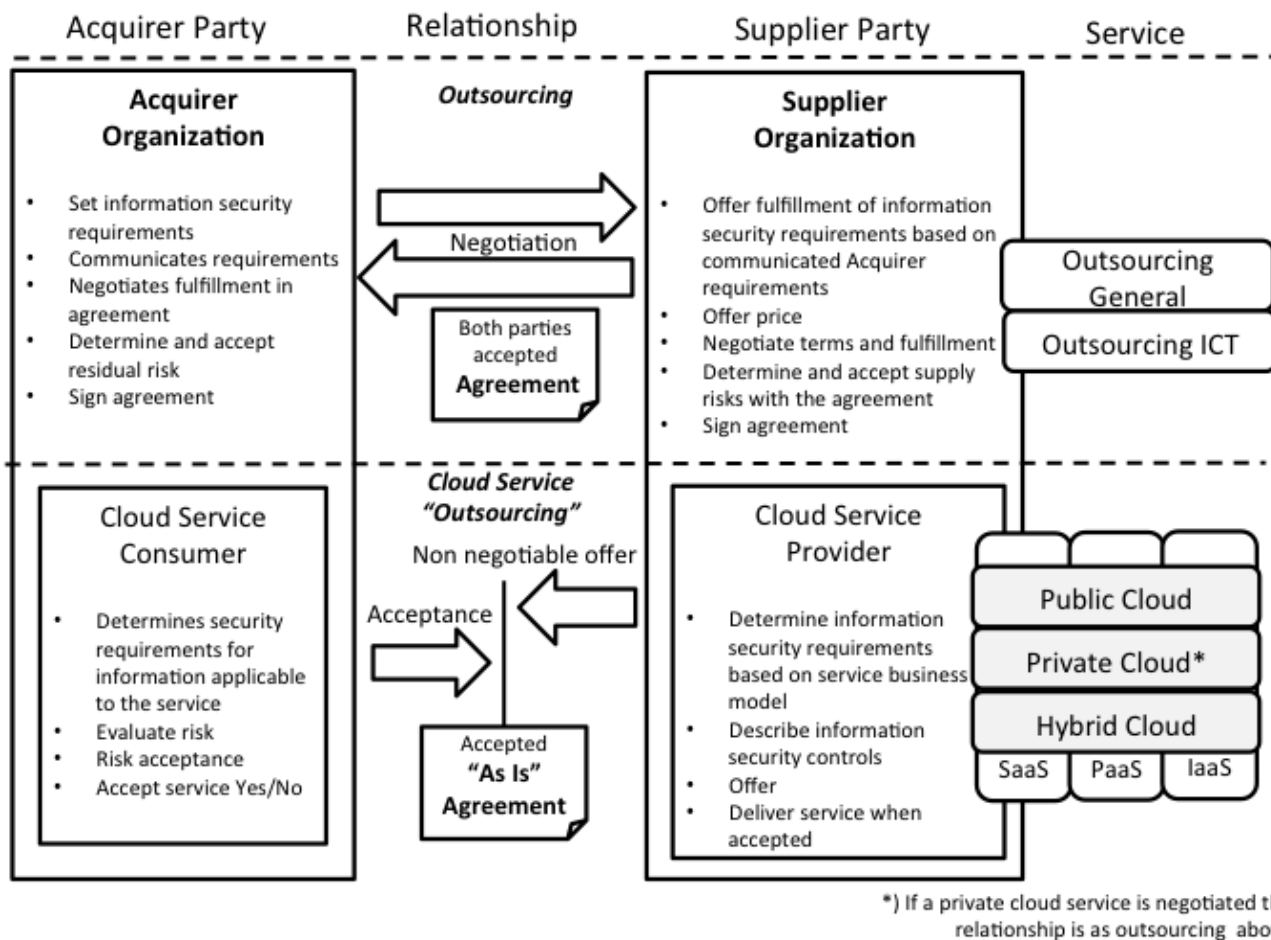


Fig 2 Principle difference in relationship between Outsourcing and Cloud Service "outsourcing"

5.2 Cloud service threats and associated risks

Use of cloud-based services presents a variety of risks to acquirers and their information, with consequences such as loss of confidentiality through accidental or intentional disclosure, loss of integrity (through, for example, insertion of malicious code), or loss of availability if a service interruption occurs.

Editors Note: Cloud service risks and threats are addressed in ISO/IEC 27017 (Annex B). *Editors request for NBs to submit contributions towards the treats and associated risks.*

6 Information security in cloud services (Consumer)

6.1 Agreement processes

6.1.1 Acquisition process

In addition to ISO/IEC 27036-3 Acquirers 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 provider;
 - 2) promises smooth communication between acquirer and supplier

- 3) defines clear demarcation of roles and responsibilities between acquirer and supplier (See ISO/IEC27017 CLD6.3.1) ;
- 4) needs least measures for mitigating cloud specific risks;
- 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 acquirer 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 acquirer and supplier;
- e) Define methods and acceptable evidence for assessing suppliers 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 supplier upon contract termination including a transition plan.

6.1.2 Supply process

Supply process is addressed in Clause 7.

6.2 Organisational project-enabling processes

For organizational project-enabling processes ISO/IEC 2703602 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 (LRP), 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

Editors' note: Editors request for NBs to submit contributions towards the cloud-specific text that needs to be addressed under technical processes. Technical processes include:

Stakeholder requirements definition process

Requirements analysis process

Architectural design process

Implementation process

Integration process

Verification process

Transition process

Validation process

Operation process

Maintenance process

Disposal process

The Editors also request that before submitting contributions experts review ISO/IEC 27036-3 to determine what is already covered and does not need to be addressed.

7 Information security controls in cloud services (provider)

7.1 Overview

A Cloud Service provider can provide increased trust to the potential and existing Cloud Service Consumers by providing information security on two viewpoints:

- a) The Cloud Service Provider as an organisation at least the part of the organisation providing the actual cloud service/-s) is aligned with ISO/IEC 27001 ISMS requirements.

- b) The actual service is aligned with a number of security controls, depending on the nature of the service and what 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 Consumer/-s Customer/-s are met. This should be communicated to the possible cloud user of the cloud service by referring to what standards and requirements the Cloud Service Provider fulfil and what responsibility the Cloud Service Provider has. But it is up to the Cloud Service Consumer Customer to accept the cloud service and its risks.

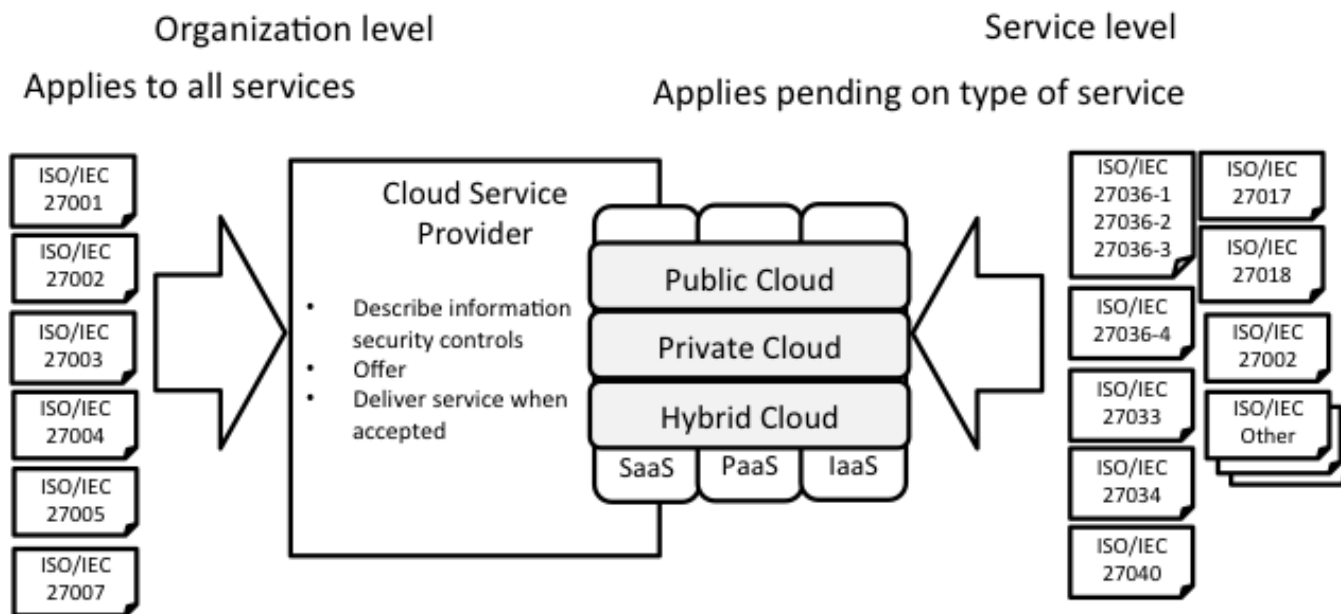


Fig 3 Extended principle use of security standards for a supplier of "Cloud" services

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 Supply process

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

- Gathering and analysis of information security specification provided by cloud service provider which includes SLA or other contract documents;
- Evaluation of cloud-specific risks (See ISO/IEC27017 5.1.1 and Annex B) based on provided information focusing on;
 - Isolation of customers in virtualized area (See ISO/IEC27017 CLD 9.5.1)
 - Operation log of privileged cloud user (See ISO/IEC27017 CLD 12.4.3)
 - Information distribution of incident.

- c) Defined policy of use of cloud computing which includes (See ISO/IEC27017 5.1.1) and
 - 1) confirm that the policy is appropriate for mitigating risks to acceptable level;
 - 2) Restrict use of cloud;
 - 3) Introduce additional controls.
- d) Methods for providing audit, assessment or reviews of the product or service to the acquirer;
- e) Evidence of secure back-up/archive capability;
- f) Evidence of business continuity and disaster recovery plans for the provided cloud-based services.

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

Annex B (informative)

XXXX

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

Annex C (informative)

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 can 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.*

Annex D
(informative)

Mapping to ISO/IEC 27017 controls

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

ISO/IEC 27036-4 Clause/Subclause	ISO/IEC 27017 Clause/Subclause

Bibliography

- [1] ISO/IEC 27018:–¹², Information technology – Security techniques – Code of practice for data protection controls for public cloud computing services
- [2] ISO/IEC 17788: –¹³, Information technology – Cloud computing – Overview and vocabulary
- [3] ISO/IEC 17789: –¹⁴, Information technology – Cloud computing – Reference architecture

¹² To be published.

¹³ To be published.

¹⁴ To be published.