INTERNATIONAL STANDARD

ISO/IEC 27036-4

First edition
2016-10-01

Information technology — Security techniques — Information security for supplier relationships —

Part 4: Guidelines for security of cloud services

Technologies de l'information — Techniques de sécurité — Sécurité d'information pour la relation avec le fournisseur —

Partie 4: Lignes directrices pour la sécurité des services du nuage

Reference number
ISO/IEC 27036-4:2016(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

A list of all parts in the ISO/IEC 27036 series can be found on the ISO website.

Introduction

This document provides guidance on information security to cloud service customers and cloud service providers. Its application should result in

— increased understanding and definition of information security in cloud services,

— increased understanding by the customers of the risks associated with cloud services to enhance the specification of information security requirements, and

— increased ability of cloud service providers to provide assurance to customers that they have identified risks in their service(s) and associated supply chains and have taken measures to manage those risks.

This document is intended to be used by all types of organizations that acquire or supply cloud services. The document is intended primarily for risk owners in cloud service customers, who finally accept the use of the cloud service, and the individual accountable for the cloud service provided by the cloud service provider. The guidance is primarily focused on the initial link of the first cloud service customer and cloud service provider, but the principal steps should be applied throughout the supply chain, starting when the first cloud service provider changes its role to being a cloud service customer 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 cloud service customer-cloud service provider link in the chain are central to this document. By following the guidance contained within this document, 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 customers and providers. ISO/IEC 27017 and ISO/IEC 27018 provide guidance on how a cloud service customer and 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. This document is based upon the premise that a cloud service customer has applied general information security according to an information security management system (ISMS) (ISO/IEC 27001). As a result, much of the content is focused on the cloud service provider and depends on the capabilities type, service category and deployment model of the actual cloud service.

Typically, cloud services are purchased “as is”; a cloud service customer has no ability to specify or request changes to the cloud service being purchased. However, in certain cases, the customer has the ability to specify the service and the detail of that service, including the information security arrangements required of the supplier. ISO/IEC 27036 is written to cover both of these eventualities. This document is written to cover the first of these eventualities and refers to ISO/IEC 27036-1, ISO/IEC 27036-2 and ISO/IEC 27036-3 for the cases when security arrangements can be specified.

For a cloud service customer, this means that when reading this document, it should be noted that it is only addressing what are cloud service-specific security processes and controls. It is assumed all other general information security processes and controls necessary for the cloud service customer organization are in place to handle information security in the cloud service to be or being used. The general information security processes and controls are found in other ISO/IEC standards and in particular ISO/IEC 27036-1, ISO/IEC 27036-2, ISO/IEC 27036-3, ISO/IEC 27017 and ISO/IEC 27018.

Information technology — Security techniques — Information security for supplier relationships —

Part 4: Guidelines for security of cloud services

1 Scope

This document provides cloud service customers and cloud service providers 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 services that can have an information security impact on organizations using these services.

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

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

The scope of this document is to define guidelines supporting the implementation of information security management for the use of cloud services.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 17788 | ITU-T Rec. Y.3500, *Information technology — Cloud computing — Overview and vocabulary*

ISO/IEC 27017 | ITU-T Rec. X.1631, *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*

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

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

ISO/IEC 27036-3, *Information technology — Security techniques — Information security in supplier relationships — Part 3: Guidelines for information and communication technology 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, ISO/IEC 27036-3 and ISO/IEC 17788 | ITU-T Rec. Y.3500 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

4 Structure of this document

This document should be used in combination with the other parts within ISO/IEC 27036. It is necessary to follow ISO/IEC 27036-1, ISO/IEC 27036-2 and ISO/IEC 27036-3 to implement the guidelines. This document should be used as additional guidelines for information security specifically addressing cloud services; security controls for cloud services are found in ISO/IEC 27017 and ISO/IEC 27018. Mapping of security controls can be found in Annex A. This document is structured to be harmonized with ISO/IEC/IEEE 15288 and ISO/IEC 12207. Clause 6 mirrors lifecycle processes provided in those two standards. This document is also harmonized with ISO/IEC 27017 and provides a mapping of ISO/IEC 27017 information security controls to the lifecycle processes in Annex B.

NOTE 1 Clause 6 is particularly applicable to public cloud deployment models.

NOTE 2 In each table presented in Clause 6, a blank column is inserted between the columns of "cloud service customer" and "cloud service provider". This blank column indicates that the guidance given for cloud service customer and cloud service provider are separate and not related.

The documents named in this document are generic and do not need to be elaborated or be separate documents. Organizations should use existing documents to integrate cloud service supply chain security.

5 Key cloud concepts and security threats and risks

5.1 Characteristics of cloud computing

According to the definition of cloud computing, underpinning the cloud capabilities types and cloud service categories are a number of technologies (such as server virtualization and Service Oriented Architecture) that enable provision of the service. These cloud services typically use shared resources in which a cloud service provider can move and process a cloud service customer's information to deliver the most efficient service at minimal cost.

ISO/IEC 17788 defines three cloud capabilities types which are typically shared and consumed by many cloud service customers in supplier relationships. The following are the defined capabilities types:

a) application;

b) infrastructure;

c) platform.

Within ISO/IEC 27036, the term "acquirer" is used to indicate a stakeholder that procures a product or service from another party and an organization; the term "supplier" is used for an individual that enters into agreement with the acquirer for the supply of a product or service, respectively. In this document, the terms cloud service customer for the acquirer and cloud service provider for the supplier are used to differentiate between the roles in supplier relationships and to highlight specific roles regarding cloud services.

There are differences and similarities in acquisition process between public cloud deployment models and ICT outsourcing as shown in Figure 1. The following highlights differences between use of cloud services based on the public cloud deployment model and other information services.

a) The cloud service is generally standardized with limited flexibility for customization;

b) The cloud service provider provides the cloud service customers with pre-determined information security controls;

c) The cloud service provider does not usually accept an audit being conducted by an individual customer;

d) The cloud service customer's information security depends on the cloud service provider's ability to implement information security in the cloud service for the customer;

e) The cloud service provider offers the service to the cloud service customer with a pre-determined agreement to be used as is without changes;

For hybrid or private cloud deployment models, these statements may not be applicable and there may be the possibility of negotiating the service provided, the information security controls to be implemented and the agreement for the use of the cloud service.

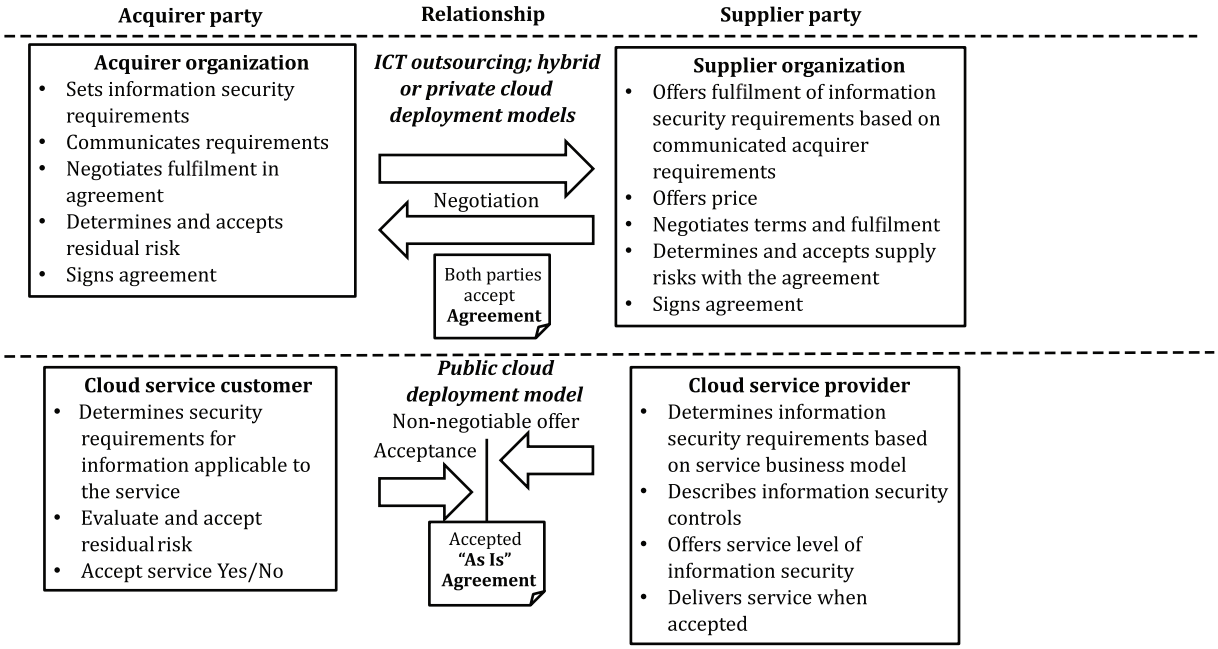

Figure 1 — Differences and similarities between ICT outsourcing and public cloud deployment models

5.2 Cloud service threats and associated risks to the cloud service customer

Cloud service customers are responsible and accountable for the information security risks incurred by the use of information system services offered by external suppliers, including cloud service providers. Cloud service customers are responsible for evaluating the risk of using a cloud service and deciding whether to use the service and selecting a specific provider. The risks related to a cloud service differ depending on the combination of cloud capabilities type, service category and deployment model. While applicable threats are similar to those related to ICT, the cloud environment changes the consequences to the cloud service customer that may result from an incident. For example, the "lack of visibility" that a cloud service customer will have into the provided service means that the customer will have increased difficulty in determining that an incident is in progress which might delay defensive measures and remediation. That would, in turn, increase the consequence (and therefore the risk) although the threat has not changed (e.g. malware attack).

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

The risks and threats depend on the factors discussed above and the sector where the cloud service and deployment model are applied. For example, there may be different risks and threats in the health care sector compared to the construction sector. Cloud service customers may require different levels of assurance depending on the risk acceptance criteria of the customer and additionally on the sector the cloud service and deployment model are applied.

Cloud service customers have limited control over the location, access, processing and protection of information placed in the cloud service. Additionally, cloud service customers may not be made aware of incidents, breaches, failures or other issues affecting the service in a timely manner. The limited control, coupled with a lack of information about the cloud service performance and security, presents a major risk of using the cloud service. When making an acquisition decision, the cloud service customer will need to evaluate these risks in relation to the information to be placed in the cloud and the dependence of the business on the information and the cloud service.

As most cloud services are not auditable by the cloud service customer, third-party assurance might be useful to evaluate and possibly reduce risks, provided that the scope of the assurance given by the third party is relevant for the actual cloud service.

5.3 Cloud service threats and associated risks for public cloud deployment model

The threats and associated risks for a cloud service customer vary among the cloud capabilities types and deployment model. Typical threats and risks for a public cloud deployment model are depicted in Table 1.

Table 1 — Typical threats and risks associated with cloud capabilities types in a public cloud deployment model

Typical threats and risks	Infrastructure capabilities type	Platform capabilities type	Application capabilities type
Lack of control on where the cloud service customer data are stored	Where cloud service customer data are stored (integrity, traceability and privacy)		
Unknown access to stored cloud service customer data	Who has access to or availability of stored cloud service customer data (availability)		
Unknown data transmission process	How cloud service customer data are communicated (confidentiality, privacy and integrity)		
Unknown superuser, administrator or privileged user access	Who has higher privileges (integrity, traceability, confidentiality and privacy)		
Lack of protection against malware	Malware, etc. (all aspects)	Malware related to unsecure platforms (all aspects)	Malware related to applications (all aspects)
Unknown access rights to cloud service customer data	*Not applicable*	Access and rights through administrator rights (confidentiality, privacy and integrity)	Access and rights through user rights (confidentiality, privacy and integrity)
Lack of log data	*Not applicable*	Lack of log data (traceability and integrity)	Lack of log data from application (traceability and integrity)
Unknown integrity of platforms	*Not applicable*	Integrity of platforms (all aspects)	
Uncontrolled application layer changes	*Not applicable*	*Not applicable*	Uncontrolled changes (integrity)
Lack of security requirement in application layer development	*Not applicable*	*Not applicable*	Lack of security requirements in development (all aspects)

Table 1 *(continued)*

Typical threats and risks	Infrastructure capabilities type	Platform capabilities type	Application capabilities type
Inability to retrieve cloud service customer data during service provision	*Not applicable*	*Not applicable*	Lack of service or other issue, stopping retrieval of cloud service customer data (availability)
Uncertainty about control over cloud service customer data during and after service provision	Poor understanding of ownership of cloud service customer data such as network traffic information (availability)	Poor understanding of ownership of cloud service customer data such as user information, etc. (availability)	Poor understanding of ownership of cloud service customer data such as user information, etc. (availability)
Inability to determine whether cloud service customer data have been completely deleted at service termination/end	Lack of assurance that cloud service customer data (such as processing, storage or networking usage) have been deleted (confidentiality and availability)	Lack of assurance that cloud service customer data (such as development versions of applications, test data and execution environments) have been deleted (confidentiality and availability)	Lack of assurance that cloud service customer data (such as application usage, type of data processed and application user data) have been deleted (confidentiality and availability)

NOTE Table 1 indicates where risks occur in a public cloud deployment model.

5.4 Cloud service threats and associated risks for hybrid cloud deployment model

Typical risks and threats listed in 5.3 apply depending on the service. Even if general security controls can be applied to a hybrid cloud service, specific cloud service information security may be needed depending on the service.

5.5 Cloud service threats and associated risks for private cloud deployment model

Typical risks and threats listed in 5.3 apply depending on the service. These risks can be adjusted through dialogue between the parties. In this dialogue, the cloud service customer can communicate their requirements for the private cloud while the cloud service provider can tailor security controls to mitigate applicable risks which will need to be accepted by the customer. It is important to consider exit controls in ISO/IEC 27002 and relevant processes in ISO/IEC 27036-3 regarding retrieving and destruction of information.

6 Information security controls in cloud service acquisition lifecycle

6.1 Agreement processes

6.1.1 Acquisition process

Cloud service customers should consider the following in their acquisition process, in addition to requirements and guidance provided in ISO/IEC 27036-2 and ISO/IEC 27036-3.

Cloud service customer		Cloud service provider
a) Establish a supplier relationship strategy to 1) Allow the customer to understand the information security in place at a particular cloud service provider. 2) Assure smooth communication between cloud service customer and cloud service provider by assigning points of contact for communication between cloud service customer and provider. 3) Define clear allocation of roles and responsibilities between cloud service customer and cloud service provider. 4) Contain guiding principles for mitigating cloud-specific risks as stated in 5.2, and 5) Extend existing security policy to cloud services.		*Not applicable*

6.1.2 Supply process

Cloud service providers should consider the following in their supply process, in addition to requirements and guidance provided in ISO/IEC 27036-2 and ISO/IEC 27036-3.

Cloud service customer		Cloud service provider
Not applicable		a) Define the scope of responsibility which the cloud service provider should accept. When the cloud service provider is a cloud service customer of other cloud services, the cloud service provider should also specify the responsibility for its use of such services. b) Declare and publish its responsibility for the cloud service that it provides. c) Provide information and functionality about the cloud service provider's protection of the cloud service customer's information. d) Disclose, if possible, the most current assurance, preferably from a third party, which ensures the reliability of the cloud service provider's protection of customer information and the certainty of the information security controls of the cloud service provider. e) Describe secure backup/archive capability of the cloud service. f) Describe resilience measures (including business continuity and disaster recovery plans) for the provided cloud services. g) State the process for notifying cloud service customers of changes in cloud service providers. h) Provide assurance evidence such as third-party audit certificates or audit/attestation reports, etc. for the cloud service. i) Establish requirements for handling multi-tenancy and for providing logical and physical separation of information for cloud service customers. j) Establish requirements for the secure transfer of cloud service customer's assets. 1) Establish requirements for restricting the movement, transmission and storage of the cloud service customer's information. 2) Define methods and acceptance criteria for assessing cloud service providers regarding the ability to provide logical and physical separation of information for cloud service customers. 3) Define processes for transition of the cloud service customer's assets to a different cloud service provider. 4) Define process for disposal or confirmation of disposal of the cloud service customer's assets in the cloud service provider's computing environment upon contract termination. k) Define processes for gathering and analysis of contractual documents related to information security of the cloud service, which can include Service Level Agreements (SLA).

6.2 Organizational 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 that 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 that 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 that provided in ISO/IEC 27036-2 and ISO/IEC 27036-3.

6.3.4 Risk management process

Cloud service customers and cloud service providers should consider the following in their risk management process, in addition to requirements and guidance provided in ISO/IEC 27036-2 and ISO/IEC 27036-3.

Cloud service customer		Cloud service provider
a) Specify the type, classification and importance of information that may be handled in the cloud (e.g. commercial information, intellectual property, legal, regulatory and privileged information, logistical information, management information or personally identifiable information). b) Specify legal/regulatory risks to the organization (e.g. copyright, information protection, financial regulation, privacy breach and corporate governance) related to the information to be handled in the cloud service. c) Evaluate risk and accept residual risk.		a) Deliver the security service levels specified in the SLA agreed with the cloud service customer. b) Manage the termination process and associated information return and/or disposal in the cloud service.

6.3.5 Configuration management process

Cloud service customers and providers should consider the following in their configuration management process, in addition to requirements and guidance provided in ISO/IEC 27036-2 and ISO/IEC 27036-3.

Cloud service customer		Cloud service provider
a) Determine the impact of changes to the service.		a) Any changes in the service should be analysed by the provider and compared to the agreed service. b) Notify cloud service customer of any changes to service.

6.3.6 Information management process

Cloud services security should be considered in this process, but there is no specific guidance in addition to that provided in ISO/IEC 27036-2 and ISO/IEC 27036-3. In addition, as part of the information management process, the guidance is that privacy of data should be considered and determined if it is applicable from both the cloud service customer and cloud service provider point of view for authentication and other relevant information processes.

The cloud service provider should especially determine if there are any identity data that are also considered as privacy information due to the technical authentication solution of the provided cloud service. This type of information is normally only known by the cloud service provider and not the cloud service customer if not communicated. The determination if authentication data are also privacy information can vary depending on different legal aspects defining data as privacy information and the actual cloud service model.

6.3.7 Measurement process

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

6.4.2 Requirements analysis process

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

6.4.3 Architectural design process

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

6.4.4 Implementation process

The following should be included as part of the implementation process to ensure that the cloud service customer and cloud service provider are appropriately managing the security risks, in addition to requirements and guidance provided in ISO/IEC 27036-2 and ISO/IEC 27036-3.

Cloud service customer			Cloud service provider
a) Implement the cloud service in a stepwise manner, especially if sensitive or critical information is to be stored or processed on a cloud service. The cloud service customer should deploy the cloud service by a phased approach in order to reduce risks. The cloud service customer should deploy a part of the cloud service which has less risk and expand the use of the service in a stepwise manner, while overviewing the situation.			a) Implement, manage and run security controls.

6.4.5 Integration process

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

6.4.6 Verification process

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

6.4.7 Transition process

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

6.4.8 Validation process

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

6.4.9 Operation process

The following should be included as part of the operation process to ensure that the cloud service customer and cloud service provider are appropriately managing the security risks, in addition to requirements and guidance provided in ISO/IEC 27036-2 and ISO/IEC 27036-3.

Cloud service customer		Cloud service provider
a) Implement a "cloud use policy" and arrange training for personnel. b) Monitor cloud service changes and address the impact of those changes. c) Collect information on and respond to information security incidents related to the cloud service.		a) Provide information and functionality that are defined in supply process to the cloud service customer. 1) Establish an operation process to provide the information and functionality appropriately to cloud service customers. 2) Provide information and functionality through the operation process. 3) Monitor to ensure that the process is operated appropriately and to evaluate the process when necessary. b) Monitor the activity of the cloud service customers within the scope of the agreement between the cloud service provider and the cloud service customer and notify the corresponding cloud service customer when the activity can affect the provision of the cloud service. c) Monitor the activity of the cloud service provider and ensure accountability of all actions done to the cloud services or the infrastructure for cloud service provisioning.

6.4.10 Maintenance process

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

6.4.11 Disposal process

Cloud service customers and cloud service providers should consider the following in their disposal process, in addition to requirements and guidance provided in ISO/IEC 27036-2 and ISO/IEC 27036-3.

Cloud service customer		Cloud service provider
a) Confirmation of information disposal at termination of service use in the cloud service.		a) Establish a process to log the information disposal when disposing of cloud service customer's assets with the consent of the cloud service customer terminating the use of the cloud service. b) Establish a process to maintain the disposal log appropriately. c) Establish a procedure to disclose disposal logs upon a request from a cloud service customer.

7 Information security controls in cloud service providers

7.1 Overview

7.1.1 Control sets related to cloud service deployment model

The controls applied to mitigate risks and threats related to a cloud service can differ depending on the combination of capabilities type, service category, deployment model and target customer profile. 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 service customer's security needs based on the industry context (sector), geography, legal context, etc. The cloud service provider should also keep in mind that while it is the customer who needs to comply with legal and regulatory requirements, the cloud service provider's ability to address this need defines the success of the provider.

The focus of Clause 7 is the control set related to the public cloud deployment model in combination with different cloud capabilities types. Specific and detailed controls can be found in other standards such as ISO/IEC 27017 or ISO/IEC 27018.

7.1.2 Setting information security controls at a cloud service provider

It is likely that the cloud service customer has already a set of requirements that has to be met. 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, and

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. How the controls are implemented should also be of concern, which should be determined by the cloud service provider and communicated to the market/intended customers. 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.

A cloud service provider can increase trust of cloud service customers (existing and potential) by articulating their information security practices as follows:

a) demonstrating alignment of the part of the organization providing the cloud service(s) with an applicable information security management standard, such as ISO/IEC 27001;

b) demonstrating alignment with applicable security controls, based on the nature of the service and the requirements of the market where the service is delivered.

The cloud service provider should communicate alignment with information security management standards and security controls to prospective cloud service customer(s). This can be accomplished by stating specific standards and controls with which the cloud service is aligned. While this alignment will reduce the risks to the cloud service customer, it will not eliminate them.

Figure 2 highlights how a cloud service provider can use information security standards to assist in protecting both the provider organization and the cloud capabilities and service categories offered to cloud service customers.

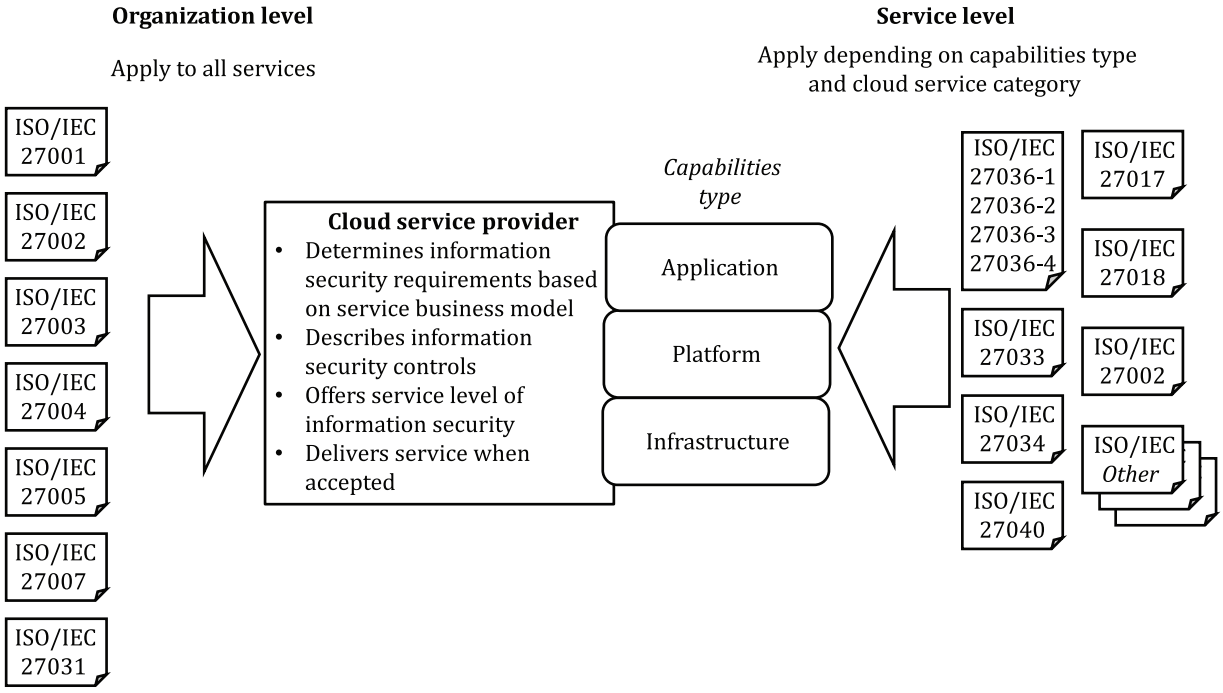

Figure 2 — Example use of security standards at a cloud service provider

For further mapping of relevant controls to cloud services and deployment models, see Annex A.

7.2 Public cloud deployment model

7.2.1 Infrastructure capabilities type

A cloud service provider should implement the controls stipulated in ISO/IEC 27002 to ensure security of the infrastructure which the cloud service provider provides to its cloud service customers.

The main controls are as follows:

a) controls for network security (including network access);

b) controls for communication security (including cryptography);

c) controls for storage security (including physical storage and security during the lifecycle);

d) malware protection;

e) monitoring;

f) capacity management;

g) identity management;

h) incident management;

i) establishment of treatment of intellectual property rights of cloud service customers in case backup services are provided.

In addition, a cloud service provider should implement controls stipulated in ISO/IEC 27017 to carry out the responsibilities shared with its cloud service customers.

7.2.2 Platform capabilities type

A cloud service provider should ensure that security of the infrastructure and platform used for the provision of platform capabilities type functionality is at the same level with its services. Additionally, a cloud service provider should perform the controls stipulated in ISO/IEC 27002 to ensure security of the platform services which the cloud service provider provides to its cloud service customers.

The main controls are as follows:

a) access controls (user and administrative access for both cloud service customer and cloud service provider);

b) management of logging;

c) controls over OS integrity;

d) controls over OS change;

e) establishment of treatment of intellectual property rights of cloud service customers in case backup services are provided.

In addition, a cloud service provider should implement controls stipulated in ISO/IEC 27017 to carry out the responsibilities shared with its cloud service customers.

7.2.3 Application capabilities type

A cloud service provider should ensure that security of the infrastructure and platform used for the provision of application capabilities type is at the same level with application services themselves. Also, a cloud service provider should perform the controls stipulated in ISO/IEC 27002 to ensure security of the application services which the cloud service provider provides to its cloud service customers.

The main controls are as follows:

a) controls for access and user rights;

b) controls for application changes;

c) controls for application services usage and transfer.

Cloud service providers should implement controls described in ISO/IEC 27017. Additional information about securing the application development lifecycle can be found in ISO/IEC 27034 (all parts).

7.3 Hybrid cloud deployment model

All the controls listed for the three cloud capabilities types above should be applied depending on the actual capabilities types and service categories in use.

7.4 Private cloud deployment model

All controls for a supplier listed in ISO/IEC 27017 apply.

Annex A
(informative)

Information security standards for cloud providers

The purpose of information security management for the cloud service customer is to protect the customer's own information consistently, regardless whether a cloud service is used or not.

On the other hand, the purpose of information security management for the cloud service provider is to provide better cloud service as well as to protect its own information. Therefore, the cloud service provider needs to expand information security measures in order to protect the information of the cloud service customer as part of service management.

Table A.1 provides cross-references for cloud services and deployment models and applicable information security and cloud security standards. When looking at platform and application capabilities types, the controls listed are assumed to be hierarchical. Some controls are directly related and some more indirectly related to the cloud capabilities type and deployment model, and Table A.1 is guidance for reviewing and determining the importance of relevant controls.

It should be noted that Table A.1 is guidance only and there may be other suitable controls and especially other standards as per the right-most column in the table ("Additional reference to other supporting ISO/IEC standards").

Table A.1 — Cross-references for cloud services and deployment models and relevant standards

Cloud capabilities type	Model	Information security subject (7.2.1 in general and 7.2.3 if stated)	ISO/IEC 27002 Control	Additional cloud-specific information or controls in ISO/IEC 27017 compared to ISO/IEC 27002	Privacy ISO/IEC 27018	Additional reference to other supporting ISO/IEC standards
Infrastructure	Public cloud	a) Controls for 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	9.2.3, 13.1.3	A.1.1, A.2.1, A.4.1, A.5.1, A.5.2, A.9.1	27032, 27033, 29115, 29003
Infrastructure	Public cloud	b) Controls for communication security (including cryptography)	10.1.1, 10.1.2, 13.1.2, 13.2.3, 18.1.5	10.1.1, 18.1.5	A.9.1	27033
Infrastructure	Public cloud	c) Controls for storage security (including physical storage and security during the lifecycle)	8.1.1, 8.1.2, 8.1.3, 8.3.2, 11.2.7, 17.2	8.1.1, 8.2.2, CLD.8.1.5	A.1.1, A.4.1, A.5.1, A.5.2	27031, 27040
Infrastructure	Public cloud	d) Malware protection	12.2.1	None	None	None
Infrastructure	Public cloud	e) Monitoring	12.4.3, 12.4.4	12.4.4	None	27033
Infrastructure	Public cloud	f) Capacity management	12.1.3	12.1.3	None	None
Infrastructure	Public cloud	g) Identity management	None	None	A.1.1, A.2.1, A.4.1, A.5.1, A.5.2, A.9.1	24760, 29115, 29003
Infrastructure	Public cloud	h) Incident management	16.1.1, 16.1.2, 16.1.4, 16.1.5, 16.1.6, 16.1.7	16.1.1, 16.1.7	A.7.1, A.9.1	27035

Table A.1 *(continued)*

Cloud capabilities type	Model	Information security subject (7.2.1 in general and 7.2.3 if stated)	ISO/IEC 27002 Control	Additional cloud-specific information or controls in ISO/IEC 27017 compared to ISO/IEC 27002	Privacy ISO/IEC 27018	Additional reference to other supporting ISO/IEC standards
Infrastructure	Public cloud	i) Establishment of treatment of intellectual property rights of cloud service customers in case backup services are provided	18.1.2	18.1.2	A.1.1, A.7.1, A.9.1	None
Platform	Public cloud	a) Access controls (user and administrative access for both cloud service customer and cloud service provider)	9.2.1, 9.2.2, 9.2.4, 9.3.1, 9.4.2, 9.4.3, 9.4.5	9.2.1, 9.2.2, 9.2.3, 9.2.4	A.1.1, A.2.1, A.4.1, A.5.1, A.5.2, A.9.1	29115, 29003
Platform	Public cloud	b) Management of logging	12.4.1, 12.4.2	12.4.1	A.1.1, A.2.1, A.5.1, A.5.2, A.9.1	None
Platform	Public cloud	c) Controls over OS integrity	12.6.1	None	None	None
Platform	Public cloud	d) Controls over OS change	12.1.1, 12.1.2, 12.5.1, 14.2.2	12.1.2	None	None
Platform	Public cloud	e) Establishment of treatment of intellectual property rights of cloud service customers in case backup services are provided	18.1.2	18.1.2	A.1.1, A.7.1, A.9.1	None
Application	Public cloud	a) Controls for access and user rights	9.4.1, 9.4.4	9.4.1, 9.4.4	A.1.1, A.2.1, A.4.1, A.5.1, A.5.2, A.9.1	27032, 29115, 29003

Table A.1 *(continued)*

Cloud capabilities type	Model	Information security subject (7.2.1 in general and 7.2.3 if stated)	ISO/IEC 27002 Control	Additional cloud-specific information or controls in ISO/IEC 27017 compared to ISO/IEC 27002	Privacy ISO/IEC 27018	Additional reference to other supporting ISO/IEC standards
Application	Public cloud	b) Controls for application changes	12.6.2	12.1.2	A.2.1, A.7.1	27032
Application	Public cloud	c) Controls for application services usage and transfer	14.1.2, 14.1.3	14.1.2, 14.1.3	A.2.1, A.2.2, A.4.1, A.5.1, A.5.2, A.7.1	27032
Application	Public cloud	7.2.3 Application development management	14.2.1, 14.2.4, 14.2.5, 14.2.6, 14.2.8, 14.2.9, 14.3.1	14.2.1	A.2.1, A.7.1	27032, 27034

Annex B
(informative)

Mapping to ISO/IEC 27017 controls

ISO/IEC 27036-4 follows the lifecycle of a cloud service. When applying controls as per ISO/IEC 27017, this annex provides guidance on when in the lifecycle process a control is applicable and also in some cases where there is no specific control suitable.

Table B.1 — Mapping of ISO/IEC 27036-4 clauses/subclauses to ISO 27017 clauses/subclauses

ISO/IEC 27036-4 clause/subclause	ISO/IEC 27017 clause/subclause (and when there is only reference in ISO/IEC 27017 to ISO/IEC 27002, this is stated)
Clause 6 Information security controls in cloud service acquisition lifecycle	
6.1 Agreement processes	Clause 5 Information security policies Clause 6 Organization of information security Clause 15 Supplier relationships Clause 18 Compliance CLD.6.3 Relationship between cloud service customer and cloud service provider
6.1.1 Acquisition process	See 6.1 mapping
6.1.2 Supply process	See 6.1 mapping
6.2 Organizational project-enabling processes	None
6.3 Project processes	
6.3.1 Project planning process	None
6.3.2 Project assessment and control process	None
6.3.3 Decision management process	None
6.3.4 Risk management process	None
6.3.5 Configuration management process	12.1.2 Change management ISO/IEC 27002, 14.2.2 System change control procedures CLD.12.1.5 Administrator's operational security
6.3.6 Information management process	8.2 Information classification 9.1 Business requirements of access control Clause 10 Cryptography 12.3 Backup ISO/IEC 27002, 13.2.1 Information transfer policies and procedures
6.3.7 Measurement process	None
6.4 Technical processes	
6.4.1 Stakeholder requirements definition process	14.1 Security requirements of information systems
6.4.2 Requirements analysis process	14.1 Security requirements of information systems
6.4.3 Architectural design process	None
6.4.4 Implementation process	14.2 Security in development and support processes

Table B.1 *(continued)*

ISO/IEC 27036-4 clause/subclause	ISO/IEC 27017 clause/subclause (and when there is only reference in ISO/IEC 27017 to ISO/IEC 27002, this is stated)
6.4.5 Integration process	14.2 Security in development and support processes
6.4.6 Verification process	14.2 Security in development and support processes ISO/IEC 27002, 14.3 Test data
6.4.7 Transition process	ISO/IEC 27002, 14.2.8 System security testing
6.4.8 Validation process	14.2 Security in development and support processes ISO/IEC 27002, 14.3 Test data
6.4.9 Operation process	Clause 8 Asset management Clause 9 Access control Clause 10 Cryptography Clause 12 Operations security Clause 13 Communications security Clause 16 Information security incident management ISO/IEC 27002, Clause 17 Information security aspects of business continuity management Clause 18 Compliance CLD.9.5 Access control of cloud service customer data in shared virtual environment CLD.9.5.2 Virtual machine hardening CLD.12.1.5 Administrator's operational security CLD.12.4.5 Monitoring of cloud services CLD.13.1.4 Alignment of security management for virtual and physical networks
6.4.10 Maintenance process	ISO/IEC 27002, 8.3 Media handling 13. Communications security ISO/IEC 27002, 17 Information security aspects of business continuity Management
6.4.11 Disposal process	Clause 8 Asset management ISO/IEC 27002, 13.2 Information transfer CLD.8.1.5 Removal of cloud service customer assets

Bibliography

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

[2] ISO/IEC 19086-1, *Information technology — Cloud computing — Service level agreement (SLA) framework and technology — Part 1: Overview and concepts*

[3] ISO/IEC 27018, *Information technology — Security techniques —Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

[4] ISO/IEC 29003,[1)]*Information technology — Security techniques — Identity proofing*

[5] ISO/IEC 29115, *Information technology — Security techniques — Entity authentication assurance framework*

1) Under development.

ICS 35.040
Price based on 21 pages