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

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.

INTERNATIONAL STANDARD ISO/IEC 27036-4:2016(E)

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.

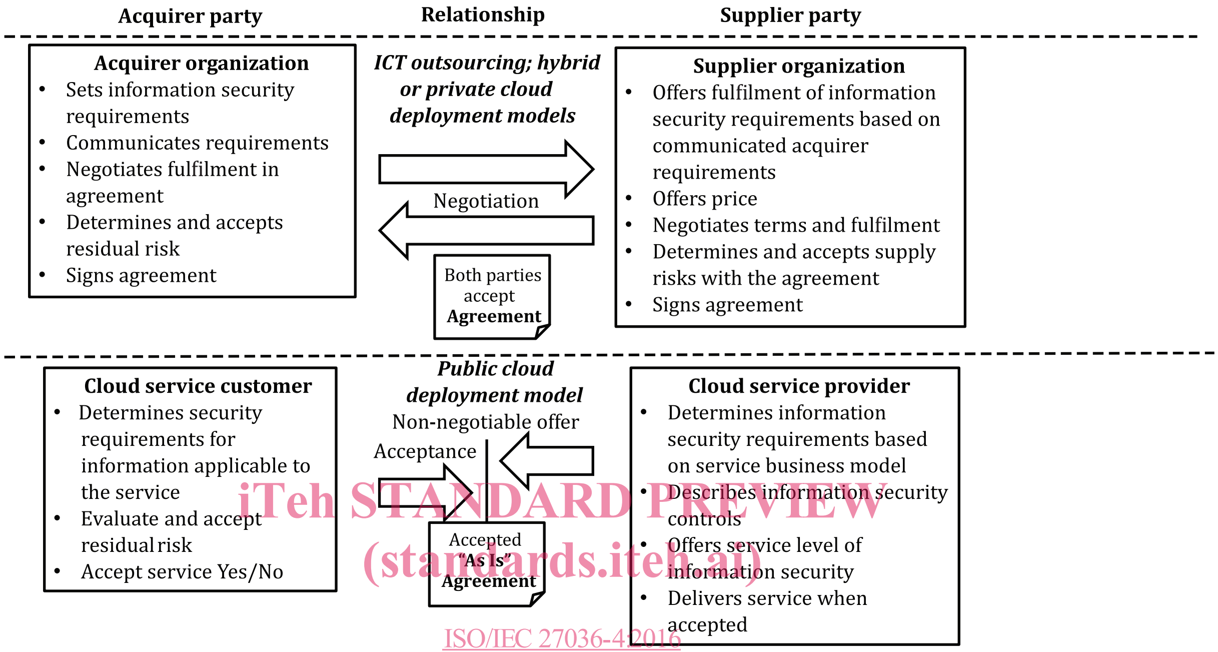
Acquirer party
Relationship
Supplier party
Acquirer organization
• Sets information security requirements
• Communicates requirements
• Negotiates fulfilment in agreement
• Determines and accepts residual risk
• Signs agreement
ICT outsourcing; hybrid or private cloud deployment models
Negotiation
Both parties accept Agreement
Supplier organization
• Offers fulfilment of information security requirements based on communicated acquirer requirements
• Offers price
• Negotiates terms and fulfilment
• Determines and accepts supply risks with the agreement
• Signs agreement
Cloud service customer
• Determines security requirements for information applicable to the service
• Evaluate and accept residual risk
• Accept service Yes/No
Public cloud deployment model
Non-negotiable offer
Acceptance
Accepted “As Is” Agreement
Cloud service provider
• Determines information security requirements based on service business model
• Describes information security controls
• Offers service level of information security
• Delivers service when accepted

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.