INTERNATIONAL STANDARD

**ISO/IEC 27017**

First edition
2015-12-15

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

*Technologies de l'information — Techniques de sécurité — Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage*



Reference number
ISO/IEC 27017:2015(E)



ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

## 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 27017 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*, in collaboration with ITU-T. The identical text is published as ITU-T. X.1631 (07/2015).

International Telecommunication Union

# ITU-T X.1631

(07/2015)

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cloud computing security – Cloud computing security design

---

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

Recommendation ITU-T X.1631

ITU-T X-SERIES RECOMMENDATIONS

**DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY**

| | |
|---|---|
| PUBLIC DATA NETWORKS | X.1–X.199 |
| OPEN SYSTEMS INTERCONNECTION | X.200–X.299 |
| INTERWORKING BETWEEN NETWORKS | X.300–X.399 |
| MESSAGE HANDLING SYSTEMS | X.400–X.499 |
| DIRECTORY | X.500–X.599 |
| OSI NETWORKING AND SYSTEM ASPECTS | X.600–X.699 |
| OSI MANAGEMENT | X.700–X.799 |
| SECURITY | X.800–X.849 |
| OSI APPLICATIONS | X.850–X.899 |
| OPEN DISTRIBUTED PROCESSING | X.900–X.999 |
| INFORMATION AND NETWORK SECURITY | |
| General security aspects | X.1000–X.1029 |
| Network security | X.1030–X.1049 |
| Security management | X.1050–X.1069 |
| Telebiometrics | X.1080–X.1099 |
| SECURE APPLICATIONS AND SERVICES | |
| Multicast security | X.1100–X.1109 |
| Home network security | X.1110–X.1119 |
| Mobile security | X.1120–X.1139 |
| Web security | X.1140–X.1149 |
| Security protocols | X.1150–X.1159 |
| Peer-to-peer security | X.1160–X.1169 |
| Networked ID security | X.1170–X.1179 |
| IPTV security | X.1180–X.1199 |
| CYBERSPACE SECURITY | |
| Cybersecurity | X.1200–X.1229 |
| Countering spam | X.1230–X.1249 |
| Identity management | X.1250–X.1279 |
| SECURE APPLICATIONS AND SERVICES | |
| Emergency communications | X.1300–X.1309 |
| Ubiquitous sensor network security | X.1310–X.1339 |
| PKI related Recommendations | X.1340–X.1349 |
| CYBERSECURITY INFORMATION EXCHANGE | |
| Overview of cybersecurity | X.1500–X.1519 |
| Vulnerability/state exchange | X.1520–X.1539 |
| Event/incident/heuristics exchange | X.1540–X.1549 |
| Exchange of policies | X.1550–X.1559 |
| Heuristics and information request | X.1560–X.1569 |
| Identification and discovery | X.1570–X.1579 |
| Assured exchange | X.1580–X.1589 |
| CLOUD COMPUTING SECURITY | |
| Overview of cloud computing security | X.1600–X.1601 |
| **Cloud computing security design** | **X.1602–X.1639** |
| Cloud computing security best practices and guidelines | X.1640–X.1659 |
| Cloud computing security implementation | X.1660–X.1679 |
| Other cloud computing security | X.1680–X.1699 |

*For further details, please refer to the list of ITU-T Recommendations.*

**INTERNATIONAL STANDARD ISO/IEC 27017**
**RECOMMENDATION ITU-T X.1631**

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


## Summary

Recommendation ITU-T X.1631 | ISO/IEC 27017 provides guidelines for information security controls applicable to the provision and use of cloud services by providing:

- additional implementation guidance for relevant controls specified in ISO/IEC 27002;
- additional controls with implementation guidance that specifically relate to cloud services.

This Recommendation | International Standard provides controls and implementation guidance for both cloud service providers and cloud service customers.





## History

| Edition | Recommendation | Approval | Study Group | Unique ID* |
|---|---|---|---|---|
| 1.0 | ITU-T X.1631 | 2015-07-14 | 17 | 11.1002/1000/12490 |


* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

## FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.



## NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

## INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

**CONTENTS**

**Introduction**

The guidelines contained within this Recommendation | International Standard are in addition to and complement the guidelines given in ISO/IEC 27002.

Specifically, this Recommendation | International Standard provides guidelines supporting the implementation of information security controls for cloud service customers and cloud service providers. Some guidelines are for cloud service customers who implement the controls, and others are for cloud service providers to support the implementation of those controls. The selection of appropriate information security controls and the application of the implementation guidance provided, will depend on a risk assessment and any legal, contractual, regulatory or other cloud-sector specific information security requirements.

**INTERNATIONAL STANDARD**
**ITU-T RECOMMENDATION**

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

## 1 Scope

This Recommendation | International Standard gives guidelines for information security controls applicable to the provision and use of cloud services by providing:

- additional implementation guidance for relevant controls specified in ISO/IEC 27002;
- additional controls with implementation guidance that specifically relate to cloud services.

This Recommendation | International Standard provides controls and implementation guidance for both cloud service providers and cloud service customers.

## 2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

### 2.1 Identical Recommendations | International Standards

- Recommendation ITU-T Y.3500 (in force) | ISO/IEC 17788: (in force), *Information technology – Cloud computing – Overview and vocabulary*.
- Recommendation ITU-T Y.3502 (in force) | ISO/IEC 17789: (in force), *Information technology – Cloud computing – Reference architecture*.

### 2.2 Additional References

- ISO/IEC 27000: (in force), *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.
- ISO/IEC 27002:2013, *Information technology – Security techniques – Code of practice for information security controls*.

## 3 Definitions and abbreviations

### 3.1 Terms defined elsewhere

For the purposes of this Recommendation | International Standard, the terms and definitions given in ISO/IEC 27000, Rec. ITU-T Y.3500 | ISO/IEC 17788, Rec. ITU-T Y.3502 | ISO/IEC 17789 and the following definitions apply:

**3.1.1** The following term is defined in ISO 19440:

- **capability**: Quality of being able to perform a given activity.

**3.1.2** The following terms are defined in ISO/IEC 27040:

- **data breach**: Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored, or otherwise processed.
- **secure multi-tenancy**: Type of multi-tenancy that employs security controls to explicitly guard against data breaches and provides validation of these controls for proper governance.

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

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

**3.1.3** The following term is defined in ISO/IEC 17203:

– **virtual machine**: The complete environment that supports the execution of guest software.

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

## 3.2 Abbreviations

For the purposes of this Recommendation | International Standard, the following abbreviations apply:

| | |
|---|---|
| IaaS | Infrastructure as a Service |
| PaaS | Platform as a Service |
| PII | Personally Identifiable Information |
| SaaS | Software as a Service |
| SLA | Service Level Agreement |
| VM | Virtual Machine |

# 4 Cloud sector-specific concepts

## 4.1 Overview

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

Users of this Recommendation | International Standard should refer to clauses 5 to 18 in ISO/IEC 27002 for controls, implementation guidance and other information. Because of the general applicability of ISO/IEC 27002, many of the controls, implementation guidance and other information apply to both the general and cloud computing contexts of an organization. For example, "6.1.2 Segregation of duties" of ISO/IEC 27002 provides a control that can be applied whether the organization is acting as a cloud service provider or not. Additionally, a cloud service customer can derive requirements for segregation of duties in the cloud environment from the same control, e.g., segregating the cloud service customers' cloud service administrators and cloud service users.

As an extension to ISO/IEC 27002, this Recommendation | International Standard further provides cloud service specific controls, implementation guidance and other information (see clause 4.5) that are intended to mitigate the risks that accompany the technical and operational features of cloud services (see Annex B). The cloud service customers and the cloud service providers can refer to ISO/IEC 27002 and this Recommendation | International Standard to select controls with the implementation guidance, and add other controls if necessary. This process can be done by performing an information security risk assessment and risk treatment in the organizational and business context where cloud services are used or provided (see clause 4.4).

## 4.2 Supplier relationships in cloud services

ISO/IEC 27002 clause 15 "Supplier relationships" provides controls, implementation guidance and other information for managing information security in supplier relationships. The provision and use of cloud services is a kind of supplier relationship, where the cloud service customer is an acquirer, and the cloud service provider is a supplier. Therefore, the clause applies to cloud service customers and cloud service providers.

Cloud service customers and cloud service providers can also form a supply chain. Suppose that a cloud service provider provides an infrastructure capabilities type service. In addition, another cloud service provider can provide an application capabilities type service. In this case, the second cloud service provider is a cloud service customer with respect to the first, and a cloud service provider with respect to the cloud service customer using its service. This example illustrates the case where this Recommendation | International Standard applies to an organization both as a cloud service customer and as a cloud service provider. Because cloud service customers and cloud service providers form a supply chain through the design and implementation of the cloud service(s), clause "15.1.3 Information and communication technology supply chain" of ISO/IEC 27002 applies.

The multi-part International Standard ISO/IEC 27036, "*Information security for supplier relationships*", provides detailed guidance on the information security in supplier relationships to the acquirer and supplier of products and services.

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

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

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

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

### 4.4 Managing information security risks in cloud services

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

In contrast to the general applicability of the information security risk management processes, cloud computing has its own types of risk sources, including threats and vulnerabilities, which are derived from its features, e.g., networking, scalability and elasticity of the system, resource sharing, self-service provisioning, administration on-demand, cross-jurisdictional service provisioning, and limited visibility into the implementation of controls. Annex B provides references that give information on these risk sources and associated risks in the provision and use of cloud services.

The controls and implementation guidance given in clauses 5 to 18 and Annex A of this Recommendation | International Standard address cloud computing specific risk sources and risks.

### 4.5 Structure of this standard

This Recommendation | International Standard is structured in a format similar to ISO/IEC 27002. This Recommendation | International Standard includes clauses 5 to 18 of ISO/IEC 27002 by stating the applicability of its texts at each clause and paragraph.

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

When an objective with controls, or a control under an objective from ISO/IEC 27002, is needed in addition to those of ISO/IEC 27002, they are given in normative Annex A: Cloud service extended control set. When a control of ISO/IEC 27002 or Annex A of this Recommendation | International Standard needs additional cloud service specific implementation guidance related to the control, it is given under the subtitle "**Implementation guidance for cloud services**". The guidance is provided in one of the following two types:

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

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

**Type 1**

| Cloud service customer | Cloud service provider |
|---|---|
| | |

**Type 2**

| Cloud service customer | Cloud service provider |
|---|---|
| | |

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

# 5 Information security policies

## 5.1 Management direction for information security

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

### 5.1.1 Policies for information security

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

**Implementation guidance for cloud services**

| Cloud service customer | Cloud service provider |
|---|---|
| An information security policy for cloud computing should be defined as a topic-specific policy of the cloud service customer. The cloud service customer's information security policy for cloud computing should be consistent with the organization's acceptable levels of information security risks for its information and other assets.<br>When defining the information security policy for cloud computing, the cloud service customer should take the following into account:<br>– information stored in the cloud computing environment can be subject to access and management by the cloud service provider;<br>– assets can be maintained in the cloud computing environment, e.g., application programs;<br>– processes can run on a multi-tenant, virtualized cloud service;<br>– the cloud service users and the context in which they use the cloud service;<br>– the cloud service administrators of the cloud service customer who have privileged access;<br>– the geographical locations of the cloud service provider's organization and the countries where the cloud service provider can store the cloud service customer data (even temporarily). | The cloud service provider should augment its information security policy to address the provision and use of its cloud services, taking the following into account:<br>– the baseline information security requirements applicable to the design and implementation of the cloud service;<br>– risks from authorized insiders;<br>– multi-tenancy and cloud service customer isolation (including virtualization);<br>– access to cloud service customer assets by staff of the cloud service provider;<br>– access control procedures, e.g., strong authentication for administrative access to cloud services;<br>– communications to cloud service customers during change management;<br>– virtualization security;<br>– access to and protection of cloud service customer data;<br>– lifecycle management of cloud service customer accounts;<br>– communication of breaches and information sharing guidelines to aid investigations and forensics. |

**Other information for cloud services**

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

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

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

### 5.1.2 Review of the policies for information security

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

# 6 Organization of information security

## 6.1 Internal organization

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

### 6.1.1 Information security roles and responsibilities

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

**Implementation guidance for cloud services**

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

**Other information for cloud services**

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

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

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

### 6.1.2 Segregation of duties

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

### 6.1.3 Contact with authorities

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

**Implementation guidance for cloud services**

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

**Other information for cloud services**

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

### 6.1.4 Contact with special interest groups

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

### 6.1.5 Information security in project management

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

## 6.2 Mobile devices and teleworking

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

### 6.2.1 Mobile device policy

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

### 6.2.2 Teleworking

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

# 7 Human resource security

## 7.1 Prior to employment

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

### 7.1.1 Screening

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

### 7.1.2 Terms and conditions of employment

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

## 7.2 During employment

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

### 7.2.1 Management responsibilities

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

### 7.2.2 Information security awareness, education and training

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

**Implementation guidance for cloud services**

| Cloud service customer | Cloud service provider |
|---|---|
| The cloud service customer should add the following items to awareness, education and training programmes for cloud service business managers, cloud service administrators, cloud service integrators and cloud service users, including relevant employees and contractors:<br>– standards and procedures for the use of cloud services;<br>– information security risks relating to cloud services and how those risks are managed;<br>– system and network environment risks with the use of cloud services;<br>– applicable legal and regulatory considerations. | The cloud service provider should provide awareness, education and training for employees, and request contractors to do the same, concerning the appropriate handling of cloud service customer data and cloud service derived data. This data can contain information confidential to a cloud service customer or be subject to specific limitations, including regulatory restrictions, on access and use by the cloud service provider. |

| Cloud service customer | Cloud service provider |
|---|---|
| Information security awareness, education and training programmes about cloud services should be provided to management and the supervising managers, including those of business units. These efforts support effective co-ordination of information security activities. | |

#### 7.2.3 Disciplinary process

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

### 7.3 Termination and change of employment

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

#### 7.3.1 Termination or change of employment responsibilities

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

## 8 Asset management

### 8.1 Responsibility for assets

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

#### 8.1.1 Inventory of assets

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

**Implementation guidance for cloud services**

| Cloud service customer | Cloud service provider |
|---|---|
| The cloud service customer's inventory of assets should account for information and associated assets stored in the cloud computing environment. The records of the inventory should indicate where the assets are maintained, e.g. identification of the cloud service. | The inventory of assets of the cloud service provider should explicitly identify:<br>– cloud service customer data;<br>– cloud service derived data. |

**Other information for cloud services**

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

#### 8.1.2 Ownership of assets

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

**Other information for cloud services**

The ownership of assets will likely vary depending on the category of the cloud service being used. Application software will belong to the cloud service customer when using a platform as a service (PaaS) or infrastructure as a service (IaaS) service, whereas for a software as a service (SaaS) service, the application software will belong to the cloud service provider.

#### 8.1.3 The acceptable use of assets

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

#### 8.1.4 Return of assets

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

## 8.2 Information classification

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

### 8.2.1 Classification of information

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

### 8.2.2 Labelling of information

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

**Implementation guidance for cloud services**

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

### 8.2.3 Handling of assets

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

## 8.3 Media handling

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

### 8.3.1 Management of removable media

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

### 8.3.2 Disposal of media

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

### 8.3.3 Physical media transfer

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

# 9 Access control

## 9.1 Business requirements of access control

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

### 9.1.1 Access control policy

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

### 9.1.2 Access to networks and network services

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

**Implementation guidance for cloud services**

| Cloud service customer | Cloud service provider |
|---|---|
| The cloud service customer's access control policy for the use of network services should specify requirements for user access to each separate cloud service that is used. | (no additional implementation guidance) |

## 9.2 User access management

The objective specified in clause 9.2 of ISO/IEC 27002 applies.

### 9.2.1 User registration and deregistration

Control 9.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

**Implementation guidance for cloud services**

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

### 9.2.2 User access provisioning

Control 9.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

**Implementation guidance for cloud services**

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

**Other information for cloud services**

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

### 9.2.3 Management of privileged access rights

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

**Implementation guidance for cloud services**

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

### 9.2.4 Management of secret authentication information of users

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

**Implementation guidance for cloud services**

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

**Other information for cloud services**

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

### 9.2.5 Review of user access rights

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

### 9.2.6 Removal or adjustment of access rights

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

## 9.3 User responsibilities

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

### 9.3.1 Use of secret authentication information

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

## 9.4 System and application access control

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

### 9.4.1 Information access restriction

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

**Implementation guidance for cloud services**

| Cloud service customer | Cloud service provider |
|---|---|
| The cloud service customer should ensure that access to information in the cloud service can be restricted in accordance with its access control policy and that such restrictions are realized. This includes restricting access to cloud services, cloud service functions, and cloud service customer data maintained in the service. | The cloud service provider should provide access controls that allow the cloud service customer to restrict access to its cloud services, its cloud service functions and the cloud service customer data maintained in the service. |

**Other information for cloud services**

The cloud computing environment includes additional areas that require access controls. As part of the cloud service or cloud service functions, access to functions and services, such as the hypervisor management functions and administrative consoles, might need additional access control.

### 9.4.2 Secure log-on procedures

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

### 9.4.3 Password management system

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

### 9.4.4 Use of privileged utility programs

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

**Implementation guidance for cloud services**

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

### 9.4.5 Access control to program source code

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

# 10 Cryptography

## 10.1 Cryptographic controls

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

### 10.1.1 Policy on the use of cryptographic controls

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

**Implementation guidance for cloud services**

| Cloud service customer | Cloud service provider |
|---|---|
| The cloud service customer should implement cryptographic controls for its use of cloud services if justified by the risk analysis. The controls should be of sufficient strength to mitigate the identified risks, whether those controls are supplied by the cloud service customer or by the cloud service provider.<br>When the cloud service provider offers cryptography, the cloud service customer should review any information supplied by the cloud service provider to confirm whether the cryptographic capabilities:<br>– meet the cloud service customer's policy requirements;<br>– are compatible with any other cryptographic protection used by the cloud service customer;<br>– apply to data at rest and in transit to, from and within the cloud service. | The cloud service provider should provide information to the cloud service customer regarding the circumstances in which it uses cryptography to protect the information it processes. The cloud service provider should also provide information to the cloud service customer about any capabilities it provides that can assist the cloud service customer in applying its own cryptographic protection. |

**Other information for cloud services**

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

### 10.1.2 Key management

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

**Implementation guidance for cloud services**

| Cloud service customer | Cloud service provider |
|---|---|
| The cloud service customer should identify the cryptographic keys for each cloud service, and implement procedures for key management.<br>Where the cloud service provides key management functionality for use by the cloud service customer, the cloud service customer should request the following information on the procedures used to manage keys related to the cloud service:<br>– type of keys;<br>– specifications of the key management system, including procedures for each stage of the key life-cycle, i.e., generating, changing or updating, storing, retiring, retrieving, retaining and destroying;<br>– recommended key management procedures for use by the cloud service customer.<br>The cloud service customer should not permit the cloud service provider to store and manage the encryption keys for cryptographic operations when the cloud service customer employs its own key management or a separate and distinct key management service. | (no additional implementation guidance) |

# 11 Physical and environmental security

## 11.1 Secure areas

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

### 11.1.1 Physical security perimeter

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

### 11.1.2 Physical entry controls

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

### 11.1.3 Securing offices, rooms and facilities

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

### 11.1.4 Protecting against external and environmental threats

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

### 11.1.5 Working in secure areas

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

### 11.1.6 Delivery and loading areas

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

## 11.2 Equipment

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

### 11.2.1 Equipment siting and protection

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

### 11.2.2 Supporting utilities

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

### 11.2.3 Cabling security

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

### 11.2.4 Equipment maintenance

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

### 11.2.5 Removal of assets

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

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

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

### 11.2.7 Secure disposal or reuse of equipment

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

**Implementation guidance for cloud services**

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

**Other information for cloud services**

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

### 11.2.8 Unattended user equipment

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

### 11.2.9 Clear desk and clear screen policy

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

## 12 Operations security

### 12.1 Operational procedures and responsibilities

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

### 12.1.1 Documented operating procedures

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

### 12.1.2 Change management

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

**Implementation guidance for cloud services**

| Cloud service customer | Cloud service provider |
|---|---|
| The cloud service customer's change management process should take into account the impact of any changes made by the cloud service provider. | The cloud service provider should provide the cloud service customer with information regarding changes to the cloud service that could adversely affect the cloud service. The following will help the cloud service customer determine the effect the changes can have on information security:<br>– categories of changes;<br>– planned date and time of the changes;<br>– technical description of the changes to the cloud service and underlying systems;<br>– notification of the start and the completion of the changes.<br>When a cloud service provider offers a cloud service that depends on a peer cloud service provider, then the cloud service provider might need to inform the cloud service customer of changes caused by the peer cloud service provider. |

**Other information for cloud services**

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

### 12.1.3 Capacity management

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

**Implementation guidance for cloud services**

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

**Other information for cloud services**

Cloud services involve resources that are under the control of the cloud service provider and made available to the cloud service customer under the terms of the master service agreement and a related SLA. These resources include software, processing hardware, data storage, and network connectivity.

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

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

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

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

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

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

## 12.2 Protection from malware

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

### 12.2.1 Controls against malware

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

## 12.3 Backup

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

### 12.3.1 Information backup

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

**Implementation guidance for cloud services**

| Cloud service customer | Cloud service provider |
|---|---|
| Where the cloud service provider provides backup capability as part of the cloud service, the cloud service customer should request the specifications of the backup capability from the cloud service provider. The cloud service customer should also verify that they meet their backup requirements.<br>The cloud service customer is responsible for implementing backup capabilities when the cloud service provider does not provide them. | The cloud service provider should provide the specifications of its backup capabilities to the cloud service customer. The specifications should include the following information, as appropriate:<br>– scope and schedule of backups;<br>– backup methods and data formats, including encryption, if relevant;<br>– retention periods for backup data;<br>– procedures for verifying integrity of backup data;<br>– procedures and timescales involved in restoring data from backup;<br>– procedures to test the backup capabilities;<br>– storage location of backups.<br>The cloud service provider should provide secure and segregated access to backups, such as virtual snapshots, if such service is offered to cloud service customers. |

**Other information for cloud services**

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

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

## 12.4 Logging and monitoring

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

### 12.4.1 Event logging

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

**Implementation guidance for cloud services**

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

**Other information for cloud services**

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

### 12.4.2 Protection of log information

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

### 12.4.3 Administrator and operator logs

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

**Implementation guidance for cloud services**

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

**Other information for cloud services**

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

### 12.4.4 Clock synchronization

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

**Implementation guidance for cloud services**

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

**Other information for cloud services**

It is necessary to consider clock synchronization of the cloud service customer's systems with cloud service provider's systems, which run the cloud services used by the cloud service customer. Without such synchronization, it can be difficult to reconcile events on the cloud service customer's systems with events on the cloud service provider's systems.

## 12.5 Control of operational software

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

### 12.5.1 Installation of software on operational systems

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

## 12.6 Technical vulnerability management

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

### 12.6.1 Management of technical vulnerabilities

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

**Implementation guidance for cloud services**

| Cloud service customer | Cloud service provider |
|---|---|
| The cloud service customer should request information from the cloud service provider about the management of technical vulnerabilities that can affect the cloud services provided. The cloud service customer should identify the technical vulnerabilities it will be responsible to manage, and clearly define a process for managing them. | The cloud service provider should make available to the cloud service customer information about the management of technical vulnerabilities that can affect the cloud services provided. |

### 12.6.2 Restrictions on software installation

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

### 12.7 Information systems audit considerations

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

#### 12.7.1 Information systems audit controls

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

## 13 Communications security

### 13.1 Network security management

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

#### 13.1.1 Network controls

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

#### 13.1.2 Security of network services

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

#### 13.1.3 Segregation in networks

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

**Implementation guidance for cloud services**

| Cloud service customer | Cloud service provider |
|---|---|
| The cloud service customer should define its requirements for segregating networks to achieve tenant isolation in the shared environment of a cloud service and verify that the cloud service provider meets those requirements. | The cloud service provider should enforce segregation of network access for the following cases:<br>– segregation between tenants in a multi-tenant environment;<br>– segregation between the cloud service provider's internal administration environment and the cloud service customer's cloud computing environment.<br>Where appropriate, the cloud service provider should help the cloud service customer verify the segregation implemented by the cloud service provider. |

**Other information for cloud services**

Laws and regulations can require the segregation of networks or the isolation of network traffic.

### 13.2 Information transfer

The objective specified in clause 13.2 of ISO/IEC 27002 applies.

#### 13.2.1 Information transfer policies and procedures

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

#### 13.2.2 Agreements on information transfer

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

#### 13.2.3 Electronic messaging

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

#### 13.2.4 Confidentiality or non-disclosure agreements

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

# 14 System acquisition, development and maintenance

## 14.1 Security requirements of information systems

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

### 14.1.1 Information security requirements analysis and specification

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

**Implementation guidance for cloud services**

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

**Other information for cloud services**

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

### 14.1.2 Securing applications services on public networks

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

### 14.1.3 Protecting application services transactions

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

## 14.2 Security in development and support processes

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

### 14.2.1 Secure development policy

Control 14.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

**Implementation guidance for cloud services**

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

**Other information for cloud services**

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

### 14.2.2 System change control procedures

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

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

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

### 14.2.4 Restrictions on changes to software packages

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

#### 14.2.5 Secure system engineering principles

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

#### 14.2.6 Secure development environment

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

#### 14.2.7 Outsourced development

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

#### 14.2.8 System security testing

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

#### 14.2.9 System acceptance testing

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

**Other information for cloud services**

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

### 14.3 Test data

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

#### 14.3.1 Protection of test data

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

## 15 Supplier relationships

### 15.1 Information security in supplier relationships

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

#### 15.1.1 Information security policy for supplier relationships

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

**Implementation guidance for cloud services**

| Cloud service customer | Cloud service provider |
|---|---|
| The cloud service customer should include the cloud service provider as a type of supplier in its information security policy for supplier relationships. This will help to mitigate risks associated with the cloud service provider's access to and management of the cloud service customer data. | (no additional implementation guidance) |

#### 15.1.2 Addressing security within supplier agreements

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

**Implementation guidance for cloud services**

| Cloud service customer | Cloud service provider |
|---|---|
| The cloud service customer should confirm the information security roles and responsibilities relating to the cloud service, as described in the service agreement. These can include the following processes:<br>– malware protection;<br>– backup;<br>– cryptographic controls;<br>– vulnerability management;<br>– incident management;<br>– technical compliance checking;<br>– security testing;<br>– auditing;<br>– collection, maintenance and protection of evidence, including logs and audit trails;<br>– protection of information upon termination of the service agreement;<br>– authentication and access control;<br>– identity and access management. | The cloud service provider should specify as part of an agreement the relevant information security measures that the cloud service provider will implement to ensure no misunderstanding between the cloud service provider and cloud service customer.<br>The relevant information security measures that the cloud service provider will implement can vary based on the type of cloud service the cloud service customer is using. |

### 15.1.3 Information and communication technology supply chain

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

**Implementation guidance for cloud services**

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

## 15.2 Supplier service delivery management

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

### 15.2.1 Monitoring and review of supplier services

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

### 15.2.2 Managing changes to supplier services

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

# 16 Information security incident management

## 16.1 Management of information security incidents and improvements

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

### 16.1.1 Responsibilities and procedures

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

**Implementation guidance for cloud services**

| Cloud service customer | Cloud service provider |
|---|---|
| The cloud service customer should verify the allocation of responsibilities for information security incident management and should ensure that it meets the requirements of the cloud service customer. | As a part of the service specifications, the cloud service provider should define the allocation of information security incident management responsibilities and procedures between the cloud service customer and the cloud service provider.<br>The cloud service provider should provide the cloud service customer with documentation covering:<br>– the scope of information security incidents that the cloud service provider will report to the cloud service customer;<br>– the level of disclosure of the detection of information security incidents and the associated responses;<br>– the target timeframe in which notifications of information security incidents will occur;<br>– the procedure for the notification of information security incidents;<br>– contact information for the handling of issues relating to information security incidents;<br>– any remedies that can apply if certain information security incidents occur. |

### 16.1.2 Reporting information security events

Control 16.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

**Implementation guidance for cloud services**

| Cloud service customer | Cloud service provider |
|---|---|
| The cloud service customer should request information from the cloud service provider about the mechanisms for:<br>– the cloud service customer to report an information security event it has detected to the cloud service provider;<br>– the cloud service provider to receive reports regarding an information security event detected by the cloud service provider;<br>– the cloud service customer to track the status of a reported information security event. | The cloud service provider should provide mechanisms for:<br>– the cloud service customer to report an information security event to the cloud service provider;<br>– the cloud service provider to report an information security event to a cloud service customer;<br>– the cloud service customer to track the status of a reported information security event. |

**Other information for cloud services**

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

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

### 16.1.3 Reporting information security weaknesses

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

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

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

### 16.1.5 Response to information security incidents

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

### 16.1.6 Learning from information security incidents

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

### 16.1.7 Collection of evidence

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

**Implementation guidance for cloud services**

| Cloud service customer | Cloud service provider |
|---|---|
| The cloud service customer and the cloud service provider should agree upon the procedures to respond to requests for potential digital evidence or other information from within the cloud computing environment. | |

# 17 Information security aspects of business continuity management

## 17.1 Information security continuity

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

### 17.1.1 Planning information security continuity

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

### 17.1.2 Implementing information security continuity

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

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

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

## 17.2 Redundancies

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

### 17.2.1 Availability of information processing facilities

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

# 18 Compliance

## 18.1 Compliance with legal and contractual requirements

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

### 18.1.1 Identification of applicable legislation and contractual requirements

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

**Implementation guidance for cloud services**

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

**Other information for cloud services**

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

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

### 18.1.2 Intellectual property rights

Control 18.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

**Implementation guidance for cloud services**

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

### 18.1.3 Protection of records

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

**Implementation guidance for cloud services**

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

### 18.1.4 Privacy and protection of personally identifiable information

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

**Other information for cloud services**

ISO/IEC 27018, Code of practice for PII protection in public clouds acting as PII processors, offers additional information on this topic.

### 18.1.5 Regulation of cryptographic controls

Control 18.1.5 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

**Implementation guidance for cloud services**

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

## 18.2 Information security reviews

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

### 18.2.1 Independent review of information security

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