



**International
Standard**

ISO/IEC 27017

**Information security, cybersecurity
and privacy protection —
Information security controls based
on ISO/IEC 27002 for cloud services**

*Sécurité de l'information, cybersécurité et protection de la vie
privée — Contrôles de sécurité de l'information fondés sur l'ISO/
IEC 27002 pour les services du nuage*

**Second edition
2026-07**



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

	Page
Foreword	vi
Introduction	vii
1 Scope	1
2 Normative references	1
3 Terms, definitions and abbreviated terms	1
3.1 Terms and definitions.....	1
3.2 Abbreviated terms.....	2
4 Guidance for using this document	2
4.1 Relation between this document and ISO/IEC 27002:2022.....	2
4.2 Structure of this document.....	3
4.3 Cloud computing specific concepts.....	3
4.3.1 Supplier relationships in cloud services.....	3
4.3.2 Relationships between CSCs and CSPs.....	3
4.3.3 Managing information security risks in cloud services.....	4
5 Cloud service specific guidance related to organizational controls	5
5.1 Policies for information security.....	5
5.2 Information security roles and responsibilities.....	6
5.3 Segregation of duties.....	6
5.4 Management responsibilities.....	6
5.5 Contact with authorities.....	6
5.6 Contact with special interest groups.....	6
5.7 Threat intelligence.....	7
5.8 Information security in project management.....	7
5.9 Inventory of information and other associated assets.....	7
5.10 Acceptable use of information and other associated assets.....	7
5.11 Return of assets.....	8
5.12 Classification of information.....	8
5.13 Labelling of information.....	8
5.14 Information transfer.....	8
5.15 Access control.....	8
5.16 Identity management.....	8
5.17 Authentication information.....	9
5.18 Access rights.....	9
5.19 Information security in supplier relationships.....	9
5.20 Addressing information security within supplier agreements.....	10
5.21 Managing information security in the ICT supply chain.....	10
5.22 Monitoring, review and change management of supplier services.....	11
5.23 Information security for use of cloud services.....	11
5.24 Information security incident management planning and preparation.....	11
5.25 Assessment and decision on information security events.....	11
5.26 Response to information security incidents.....	12
5.27 Learning from information security incidents.....	12
5.28 Collection of evidence.....	12
5.29 Information security during disruption.....	12
5.30 ICT readiness for business continuity.....	12
5.31 Legal, statutory, regulatory and contractual requirements.....	13
5.32 Intellectual property rights.....	14
5.33 Protection of records.....	14
5.34 Privacy and protection of PII.....	14
5.35 Independent review of information security.....	14
5.36 Compliance with policies, rules and standards for information security.....	15
5.37 Documented operating procedures.....	15
5.38 CLD - Shared roles and responsibilities within a cloud computing environment.....	15

5.39	CLD - Agreement on the roles and responsibilities of the cloud service partner	16
6	Cloud service specific guidance related to people controls	17
6.1	Screening	17
6.2	Terms and conditions of employment	18
6.3	Information security awareness, education and training	18
6.4	Disciplinary process	18
6.5	Responsibilities after termination or change of employment	18
6.6	Confidentiality or non-disclosure agreements	18
6.7	Remote working	18
6.8	Information security event reporting	19
7	Cloud service specific guidance related to physical controls	19
7.1	Physical security perimeters	19
7.2	Physical entry	19
7.3	Securing offices, rooms and facilities	19
7.4	Physical security monitoring	19
7.5	Protecting against physical and environmental threats	19
7.6	Working in secure areas	19
7.7	Clear desk and clear screen	19
7.8	Equipment siting and protection	19
7.9	Security of assets off-premises	20
7.10	Storage media	20
7.11	Supporting utilities	20
7.12	Cabling security	20
7.13	Equipment maintenance	20
7.14	Secure disposal or re-use of equipment	20
8	Cloud service specific guidance related to technological controls	20
8.1	User endpoint devices	20
8.2	Privileged access rights	21
8.3	Information access restriction	21
8.4	Access to source code	21
8.5	Secure authentication	21
8.6	Capacity management	22
8.7	Protection against malware	22
8.8	Management of technical vulnerabilities	22
8.9	Configuration management	23
8.10	Information deletion	23
8.11	Data masking	24
8.12	Data leakage prevention	24
8.13	Information backup	24
8.14	Redundancy of information processing facilities	25
8.15	Logging	25
8.16	Monitoring activities	26
8.17	Clock synchronization	26
8.18	Use of privileged utility programs	27
8.19	Installation of software on operational systems	27
8.20	Network security	27
8.21	Security of network services	27
8.22	Segregation of networks	28
8.23	Web filtering	28
8.24	Use of cryptography	28
8.25	Secure development life cycle	28
8.26	Application security requirements	29
8.27	Secure system architecture and engineering principles	29
8.28	Secure coding	29
8.29	Security testing in development and acceptance	29
8.30	Outsourced development	29
8.31	Separation of development, test and production environments	29

ISO/IEC 27017:2026(en)

8.32	Change management.....	29
8.33	Test information.....	30
8.34	Protection of information systems during audit and testing.....	30
8.35	CLD - Segregation in virtual computing environments.....	30
8.36	CLD - Detection and prevention of unauthorized use of cloud services.....	31
Annex A (Informative) Correspondence between this document and the first edition (ISO/IEC 27017:2015).....		33
Annex B (informative) Monitoring of cloud services.....		38
Bibliography.....		39

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.

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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and <https://patents.iec.ch>. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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

For an explanation of the voluntary nature of standards, 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 www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*, in collaboration with ITU-T (as Rec. ITU-T X.1631), and in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/CLC/JTC 13, *Cybersecurity and Data Protection*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This second edition cancels and replaces the first edition (ISO/IEC 27017:2015 | Rec. ITU-T X.1631:2015), which has been technically revised.

The main changes are as follows:

- the title and the scope have been modified;
- the structure of the document has been changed, presenting the controls using a simple taxonomy and associated attributes;
- some controls have been merged, some have been removed and several new controls have been introduced.

This document has been given the status of a horizontal document in accordance with the ISO/IEC Directives, Part 1.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

The guidance contained within this document is aligned with and complements the guidance given in ISO/IEC 27002.

Specifically, this document provides guidance supporting the implementation of information security controls for cloud service customers (CSCs) and cloud service providers (CSPs). Some guidance is intended for CSCs who implement the controls and other guidance is for CSPs to support the implementation of those controls. The determination of the appropriate information security controls and the extent of the utilization of the guidance provided depends on the results of the relevant risk assessment and the existence of any legal, regulatory, contractual, or other cloud-computing specific information security requirements.

Information security, cybersecurity and privacy protection — Information security controls based on ISO/IEC 27002 for cloud services

1 Scope

This document provides guidance for information security controls, based on ISO/IEC 27002, applicable to the provision and use of cloud services. This document provides:

- additional guidance for relevant controls specified in ISO/IEC 27002:2022;
- additional controls with guidance that specifically relate to cloud services.

This document provides controls and guidance for cloud service customers (CSCs) and cloud service providers (CSPs).

This document is considered to be a horizontal document as it provides a foundation and a common understanding of security regarding the provision and use of cloud services.

NOTE This document applies to all types of cloud deployment models including the private cloud. When applying this document to the private cloud, the controls and guidance of this document are applicable, although adjustments can be necessary to adapt to the relationships and abilities of an organization's internal departments.

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 22123-1, *Information technology — Cloud computing — Part 1: Vocabulary*

ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection — Information security controls*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27002, ISO/IEC 22123-1 and the following apply.

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

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

3.1.1

capability

ability to perform a specific activity

[SOURCE: ISO 19440:2020, 3.5]

3.2 Abbreviated terms

API	application programming interface
CSC	cloud service customer
CSN	cloud service partner
CSP	cloud service provider
CSU	cloud service user
IaaS	infrastructure as a service
ICT	information and communication technology
PaaS	platform as a service
PII	personally identifiable information
RTO	recovery time objective
RPO	recovery point objective
SaaS	software as a service
SLA	service level agreement

4 Guidance for using this document

4.1 Relation between this document and ISO/IEC 27002:2022

This document provides:

- additional guidance for relevant controls specified in ISO/IEC 27002:2022;
- additional controls with guidance that specifically relate to cloud services.

This document refers to the attributes, controls, purposes, guidance and other information from ISO/IEC 27002:2022, Clauses 5 to 8. Owing to the general applicability of ISO/IEC 27002:2022, many of the controls, guidance and other information apply to both the general and cloud computing contexts of an organization. For example, ISO/IEC 27002:2022, 5.3, “Segregation of duties” provides a control that can be applied whether the organization is acting as a CSP or not. Additionally, a CSC can derive requirements for segregation of duties in the cloud computing environment from the same control, e.g. a CSC segregating the CSCs' cloud service administrators from other CSUs.

This document also provides attributes, controls, purposes, guidance and other information that are specific to cloud services and are intended to mitigate the risks that accompany the technical and operational features of cloud services (see [5.38](#), [5.39](#), [8.35](#) and [8.36](#)). [Annex A](#) provides the mappings between the set of controls of this document and the previous edition (ISO/IEC 27017:2015¹⁾).

The CSCs and the CSPs can refer to ISO/IEC 27002:2022 and this document to identify guidance on general and cloud service specific controls as 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 [4.3.3](#)).

1) Cancelled and replaced by this document (ISO/IEC 27017:2026).

4.2 Structure of this document

This document follows the structure used in ISO/IEC 27002:2022 for the description of controls.

This document adapts the information security controls included in ISO/IEC 27002:2022, Clauses 5 to 8 to better fit cloud computing. As in ISO/IEC 27002:2022, the categorization of controls given in [Clauses 5 to 8](#) is referred to as themes and the attributes of each control identified in ISO/IEC 27002:2022 also apply.

When controls specified in ISO/IEC 27002:2022 are applicable to both the CSCs and the CSP without a need for any additional information, only a reference to ISO/IEC 27002:2022 is provided.

In addition to the controls of ISO/IEC 27002:2022, cloud service extended controls are prefixed with “CLD” (CLoud service extended controls). When a control specified in ISO/IEC 27002:2022 needs additional guidance that is specific to cloud services related to the control, it is given as “guidance for cloud services”. The guidance is provided in one of the following two types:

- Type 1 (shown in [Table 1](#)), used when there is separate guidance for the CSC and the CSP;
- Type 2 (shown in [Table 2](#)), used when the guidance is the same for both the CSC and the CSP.

Table 1 — Type 1

CSC	CSP
CSC guidance	CSP guidance

Table 2 — Type 2

CSC	CSP
CSC and CSP guidance	

4.3 Cloud computing specific concepts

4.3.1 Supplier relationships in cloud services

ISO/IEC 27002:2022, 5.19 to 5.22 provide controls, the purpose of each control, guidance and other information for managing information security in supplier relationships. The provision and use of cloud services is similar to a supplier relationship, where the CSC is an acquirer and the CSP is a supplier. Therefore, ISO/IEC 27002:2022, 5.19 to 5.22 apply to CSCs and CSPs.

CSCs and CSPs can also form a supply chain. For example, a CSP provides a cloud service of infrastructure capabilities type. On top of this service, another CSP can provide a cloud service of application capabilities type. In this case, the second CSP is a CSC with respect to the first, and a CSP with respect to the CSC using its service. In this scenario, the organization has both CSC and CSP roles. Every organization should consider which controls are applicable to it in its roles as the CSC and the CSP. This example illustrates the case where this document applies to an organization both as a CSC and as a CSP. Since CSCs and CSPs form a supply chain through the provision and use of the cloud service, ISO/IEC 27002:2022, 5.21 applies as it covers the management of information security in the ICT supply chain.

The ISO/IEC 27036 series provides detailed guidance on the information security in supplier relationships to the acquirer and supplier of products and services. ISO/IEC 27036-4 deals directly with information security of cloud services in supplier relationships. ISO/IEC 27036-4 is also applicable to CSCs as acquirers and CSPs as suppliers.

4.3.2 Relationships between CSCs and CSPs

In the cloud computing environment, CSC data are stored, transmitted and processed by a cloud service. Therefore, a CSC's business processes depend upon the information security of the cloud service. Without sufficient control over the cloud service, it can be necessary for the CSC to take extra precautions with its own information security practices.

Before entering into a supplier relationship, the CSC is expected to select a cloud service, taking into account the possible gaps between the CSC's information security requirements and the information security capabilities offered by the service. Once a cloud service is selected, the CSC should manage the use of the cloud service in such a way as to meet its own information security requirements. In this relationship, collaborative effort between the CSC and the CSP for the use and provision of the cloud service is necessary for the CSC to achieve its objectives for information security management. It includes shared roles and responsibilities between the CSC and the CSP. The CSP should provide the information and technical support that are necessary to meet the CSC's information security requirements. When the information security controls provided by the CSP are pre-set and cannot be changed by the CSC, it is possible that the CSC implements additional controls of its own to mitigate risks. More information on allocation of the shared roles and responsibilities can be found in [5.38](#).

It is important to understand that there are different cloud deployment models that are used in cloud computing environments. Some of the cloud deployment models include:

- private cloud;
- public cloud;
- multi-cloud;
- federated cloud;
- hybrid cloud;
- hybrid multi-cloud;
- inter-cloud.

There are three fundamental approaches that can be taken in these different cloud deployment models.

- The CSC controls and manages the cloud services that are being delivered by each of the CSPs including their orchestration into a cloud solution (e.g. multi-cloud).
- One CSP combines cloud services from multiple CSPs with varying degrees of orchestration, control and management activities (e.g. inter-cloud).
- Multiple CSPs form a partnership through out-of-band collaboration and share their resources to create cloud services (e.g. federated cloud which uses a cloud service federation management system to orchestrate access to the CSPs resources).

It is important to note that these approaches are not mutually exclusive and it is possible to combine them. Further explanation of these cloud deployment models can be found in ISO/IEC 5140.

4.3.3 Managing information security risks in cloud services

CSCs and CSPs should both have information security risk management processes in place. They can refer to ISO/IEC 27001 for the requirements related to risk management for information security management systems, and to ISO/IEC 27005 for further guidance on information security risk management itself. ISO 31000, to which ISO/IEC 27001 and ISO/IEC 27005 are aligned, can also help with a general understanding of risk management.

The controls and guidance provide CSCs with:

- guidance on information security measures relating to the use of cloud services;
- guidance on information and capabilities of the cloud services to be obtained from CSPs.

The controls and guidance also cover how CSPs can provide information and capabilities as a part of cloud services to support CSCs' information security risk management. The information and capabilities can be provided in agreements and other documents available for CSCs.

5 Cloud service specific guidance related to organizational controls

5.1 Policies for information security

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.1 apply. In addition, the following guidance shown in [Table 3](#) and other information for cloud services also apply.

a) Guidance for cloud services

Table 3 — Guidance for policies for information security

CSC	CSP
An information security policy on the use of cloud services should be defined as a topic-specific policy of the CSC. The CSC's information security policy on the use of cloud services should be consistent with the organization's acceptable levels of information security risks for its information and other associated assets. When defining the information security policy on the use of cloud services, the CSC should take the following into account: — information stored in the cloud computing environment subject to access and management by the CSP; — assets maintained in the cloud computing environment, e.g. virtual machine instances, cloud storage buckets; — processes run on a multi-tenant, virtualized cloud service; — access level of the CSUs and the context in which they use the cloud service; — the cloud service administrators of the CSC who have privileged access; — the geographical locations of the CSP's organization and the countries where the CSP can store and process the CSC data and cloud service derived data (even temporarily); — the possibility of unauthorized uses of cloud services.	Rules for the provision of the cloud service should be defined to support the information security of the CSC, address the provision and use of its cloud services taking the following into account: — the baseline information security requirements applicable to the design and implementation of the cloud service; — multi-tenancy and CSC isolation; — virtualization of resources including servers, containers, and networks; — access to the CSC data and cloud service derived data by the personnel of the CSP; — access control procedures, e.g. strong authentication for administrative access to cloud services; — life cycle management of CSC accounts; — communications to CSCs during change management; — communication of breaches and information sharing guidelines to aid investigations and forensics.

b) Other information for cloud services

The information security policy for the use of cloud services of the CSC is one of the topic-specific policies described in ISO/IEC 27002:2022, 5.1. 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 CSC. An organization's information can be stored and maintained in the cloud computing environment, and the business processes take into consideration the cloud computing environment. General information security requirements stated in the information security policy at the top level are followed by the topic-specific policy on the use of cloud services.

In contrast to this, the rules for provision of cloud services deal with the CSCs' information and business processes, not with the CSP's information and business processes. The rule should address information security in the cloud service environment and provision of functions and information supporting the CSCs'

information security. Information security requirements for the provision of the cloud service should meet those of the prospective CSCs.

Virtualization of resources in cloud computing has several aspects that can have impacts on the CSC's information security. Examples of the aspects are:

- life cycle management of virtual instances;
- management of using virtualized images;
- handling of dormant or offline virtual instances;
- specification of snapshots;
- controlling the use of self-service portals;
- protection of hypervisors.

5.2 Information security roles and responsibilities

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.2 apply. In addition, the following guidance shown in Table 4 and other information for cloud services also apply.

a) Guidance for cloud services

Table 4 — Guidance for information security roles and responsibilities

CSC	CSP
The CSC should define information security roles and responsibilities for the use of cloud services and document them in the topic-specific policies and procedures. The CSC should allocate the roles and responsibilities and make relevant CSUs aware of them.	The CSP should define and allocate information security roles and responsibilities that relate to the provision of the cloud service.

b) Other information for cloud services

ISO/IEC 22123-3 defines roles and sub-roles of the CSC and the CSP.

5.3 Segregation of duties

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.3 apply.

5.4 Management responsibilities

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.4 apply.

5.5 Contact with authorities

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.5 apply.

5.6 Contact with special interest groups

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.6 apply.

5.7 Threat intelligence

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.7 apply. In addition, the following guidance shown in Table 5 also applies.

- a) Guidance for cloud services

Table 5 — Guidance for threat intelligence

CSC	CSP
The CSC should identify information related to information security threats on cloud computing environments and utilize them in their threat intelligence activities. The information or its sources can be provided by the CSP.	The CSP should make information related to information security threats on cloud computing environments available to the CSCs to improve its overall threat intelligence processes.

5.8 Information security in project management

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.8 apply. In addition, the following guidance for cloud services shown in Table 6 also applies.

- a) Guidance for cloud services

Table 6 — Guidance for information security in project management

CSC	CSP
The CSC should identify its information security requirements and determine if the CSP's services address those requirements. The CSC should evaluate the information from the CSP periodically while using the cloud service and review the relevant information security capabilities.	The CSP should provide information to the CSCs about the information security capabilities used by the CSC. This information should be informative without disclosing information that can be useful to someone with malicious intent.

5.9 Inventory of information and other associated assets

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.9 apply. In addition, the following guidance shown in Table 7 and other information for cloud services also apply.

- a) Guidance for cloud services

Table 7 — Guidance for inventory of information and other associated assets

CSC	CSP
The CSC's inventory should account for information and other 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, geographical location.	The inventory of information and other associated assets of the CSP should explicitly identify: — CSC data; — cloud service derived data.

- b) Other information for cloud services

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

The ownership of assets likely varies depending on the category of the cloud service being used. Application software belongs to the CSC when using a PaaS or IaaS, whereas for a SaaS, the application software belongs to the CSP.

5.10 Acceptable use of information and other associated assets

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.10 apply.

5.11 Return of assets

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.11 apply. In addition, the following guidance shown in [Table 8](#) and other information for cloud services also apply.

a) Guidance for cloud services

Table 8 — Guidance for return of assets

CSC	CSP
Before starting to use a cloud service, the CSC should confirm if its own assets on the cloud computing environment will be returned upon termination of use of the cloud service. The assets can include cloud service derived data.	The CSP should clearly state to the CSC if the CSC's assets on the cloud service, including cloud service derived data, will be returned or not upon termination of the use of the cloud service by the CSC. The CSP should return the CSC's assets when requested according to the agreements.

b) Other information for cloud services

See also [8.10](#) for the case where information deletion is required.

5.12 Classification of information

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.12 apply.

5.13 Labelling of information

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.13 apply. In addition, the following guidance for cloud services shown in [Table 9](#) also applies.

a) Guidance for cloud services

Table 9 — Guidance for labelling of information

CSC	CSP
The CSC should label information and other associated assets maintained in the cloud computing environment according to the CSC's procedures for labelling. Where applicable, functionality provided by the CSP that supports labelling can be adopted.	The CSP should document and disclose any service functionality it provides allowing CSCs to label their information and other associated assets.

5.14 Information transfer

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.14 apply.

5.15 Access control

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.15 apply.

5.16 Identity management

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.16 apply. In addition, the following guidance shown in [Table 10](#) and other information for cloud services also apply.

a) Guidance for cloud services

Table 10 — Guidance for identity management

CSC	CSP
The CSC should verify that user identity management functions and specifications provided by the CSP meet the requirements for managing access to the cloud services by the CSC's CSU.	To manage access to the cloud services by the CSC's CSU, the CSP should provide user identity management functions, and specifications for the use of these functions to the CSC.

b) Other information for cloud services

The CSP can 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 management between the CSC's systems and the cloud service, and can ease the use of multiple cloud services, supporting such capabilities as single sign-on.

5.17 Authentication information

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.17 apply. In addition, the following guidance for cloud services shown in [Table 11](#) also applies.

a) Guidance for cloud services

Table 11 — Guidance for authentication information

CSC	CSP
The CSC should verify that the CSP's procedure for managing authentication information, such as passwords, PINs, security tokens, one-time-passwords and biometrics meets the CSC's requirements.	The CSP should provide information on procedures it provides for the management of the authentication information of the CSC, including the procedures for allocating such information.

5.18 Access rights

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.18 apply. In addition, the following guidance for cloud services shown in [Table 12](#) also applies.

a) Guidance for cloud services

Table 12 — Guidance for access rights

CSC	CSP
The CSC should verify that the functions and specifications for managing the access rights of the CSC's CSUs provided by the CSP meet its requirements.	The CSP should provide functions for managing the access rights of the CSC's CSUs, and specifications for the use of these functions.

5.19 Information security in supplier relationships

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.19 apply.

5.20 Addressing information security within supplier agreements

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.20 apply. In addition, the following guidance for cloud services shown in [Table 13](#) also applies.

a) Guidance for cloud services

Table 13 — Guidance for addressing information security within supplier agreements

CSC	CSP
The CSC should ensure that the service agreement includes the information security roles and responsibilities relating to the cloud service. These can include the following: — authentication and access control; — identity and access management; — protection against malware; — vulnerability management; — backup; — collection, maintenance and protection of evidence, including logs and audit trails; — continuous monitoring; — cryptographic control; — security testing; — incident management; — technical compliance review; — auditing; — protection of information upon termination of the service agreement.	The CSP should specify as part of an agreement the relevant information security measures that the CSP implements. The relevant information security measures that the CSP will implement can vary based on the type of cloud service the CSC is using. The CSP should describe the information security roles and responsibilities related to the cloud service in the service agreement. These can include the following: — authentication and access control; — identity and access management; — protection against malware; — vulnerability management; — backup; — collection, maintenance and protection of evidence, including logs and audit trails; — continuous monitoring; — cryptographic control; — security testing; — incident management; — technical compliance review; — auditing; — protection of information upon termination of the service agreement.

5.21 Managing information security in the ICT supply chain

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.21 apply. In addition, the following guidance for cloud services shown in [Table 14](#) also applies.

a) Guidance for cloud services

Table 14 — Guidance for managing information security in the ICT supply chain

CSC	CSP
(no additional guidance)	If the CSP uses cloud services of secondary CSPs, it should ensure information security levels to its own CSCs are maintained or exceeded. When the CSP provides cloud services based on a supply chain, the CSP should provide information security objectives to suppliers, and request each of the suppliers to perform risk management activities to achieve the objectives.

5.22 Monitoring, review and change management of supplier services

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022 5.22 apply.

5.23 Information security for use of cloud services

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.23 apply.

5.24 Information security incident management planning and preparation

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.24 apply. In addition, the following guidance for cloud services shown in [Table 15](#) also applies.

a) Guidance for cloud services

Table 15 — Guidance for information security incident management planning and preparation

CSC	CSP
The CSC should request information about the allocation of responsibilities, the process and the procedures for information security incident management. The CSC should verify the following: — the scope of information security incidents that will be reported by the CSP; — the target time period in which notifications of information security incidents will be provided by the CSP; — the procedure for the notification of information security incidents from the CSP to the CSC; — contact information for the handling of issues relating to information security incidents; — any remedies that can be applied if certain information security incidents occur.	As a part of the service specifications, the CSP should define the allocation of information security incident management responsibilities and procedures between the CSC and the CSP. The CSP should provide the CSC with documentation covering: — the scope of information security incidents that the CSP will report to the CSC; — the level of disclosure of the detection of information security incidents and the associated responses; — the target time period in which notifications of information security incidents will occur; — the procedure for the notification of information security incidents; — contact information for the handling of issues relating to information security incidents; — any remedies that can be applied if certain information security incidents occur.

5.25 Assessment and decision on information security events

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.25 apply.

5.26 Response to information security incidents

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.26 apply.

5.27 Learning from information security incidents

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.27 apply.

5.28 Collection of evidence

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.28 apply. In addition, the following guidance shown in [Table 16](#) also applies.

- a) Guidance for cloud services

Table 16 — Guidance for collection of evidence

CSC	CSP
The CSC and the CSP should agree upon the procedures to respond to requests for potential digital evidence or other information related to the cloud computing environment.	

5.29 Information security during disruption

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.29 apply.

5.30 ICT readiness for business continuity

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.30 apply. In addition, the following guidance shown in [Table 17](#) and other information for cloud services also apply.

- a) Guidance for cloud services

Table 17 — Guidance for ICT readiness for business continuity

CSC	CSP
The CSC should ensure that: — the service level regarding service interruption or disruption of the cloud service which are defined in a cloud SLA or other agreements meets the RTO determined by the CSC; — the cloud service's backup functionality provided for the CSC can support the RPO for data recovery required for the CSC's ICT strategy in the event of business interruption or disruption. The CSC should consider redundancy, such as using other cloud services or ICT environments.	The CSP should provide the CSC with cloud SLA and other agreements. The CSP should provide the CSC with information and constraints related to ICT readiness for business continuity of the cloud services.

- b) Other information for cloud services

The ISO/IEC 19086 series provides information on cloud SLAs.

5.31 Legal, statutory, regulatory and contractual requirements

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.31 apply. In addition, the following guidance shown in Table 18 and other information for cloud services also apply.

a) Guidance for cloud services

Table 18 — Guidance for legal, statutory, regulatory and contractual requirements

CSC	CSP
The CSC should identify laws and regulations governing the cloud service, and evaluate if they are consistent with the obligations of the CSC. The CSC should request evidence of the CSP's compliance with relevant laws and regulations and standards required for the CSC's business. Such evidence can include assessment reports or certifications produced by third-party conformity assessment bodies. The CSC should verify that the set of cryptographic controls applied by the CSP comply with the agreements, legislation and regulations applicable to the CSC.	The CSP should provide the CSC with: — information of legal requirements for the CSP, if appropriate; — evidence of its current compliance with applicable legislation and contractual requirements; — descriptions of the cryptographic controls the CSP has implemented; — information of legal jurisdictions governing the cloud service; — geographical locations of the CSP's organization and the countries where the CSP can store and process the CSC data and cloud service derived data. The CSP should conduct a legal assessment to assess investigation requests from authorities. The legal assessment should determine whether the authority has an applicable and legally valid basis for the request and what additional steps are required. The CSP should inform the affected CSCs about investigation requests, except if the applicable legal basis of the request prohibits this or if there are clear indications of illegal actions associated with the use of the cloud service. The CSP should only grant access to or disclose the CSC's data in the context of the investigation request from the authority after the CSP's legal assessment has shown that an applicable and valid legal basis exists. The CSP should document and implement procedures to limit the access to the CSC's data by the authorities to only address the investigation request and not by default to all the CSCs' data.

b) Other information for cloud services

Information about geographical locations where the CSC data can be stored, processed or transmitted can help the CSC in determining the supervisory authorities, jurisdictions and applicable legal and regulatory requirements.

5.32 Intellectual property rights

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.32 apply. In addition, the following guidance shown in [Table 19](#) also applies.

- a) Guidance for cloud services

Table 19 — Guidance for intellectual property rights

CSC	CSP
Installing commercially licensed software in a cloud service can cause a breach of the licence terms for the software. The CSC should identify 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 CSP should establish a process for responding to intellectual property rights complaints.

5.33 Protection of records

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.33 apply. In addition, the following guidance shown in [Table 20](#) also applies.

- a) Guidance for cloud services

Table 20 — Guidance for protection of records

CSC	CSP
The CSC should request information from the CSP about the protection of records gathered, stored, and archived by the CSP related to the use of cloud services by the CSC.	The CSP should provide information to the CSC about the protection of records gathered, stored, and archived by the CSP related to the use of cloud services by the CSC.

5.34 Privacy and protection of PII

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.34 apply. In addition, the following other information for cloud services also applies.

- a) Other information for cloud services

See ISO/IEC 27018 for additional information on this topic.

5.35 Independent review of information security

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.35 apply. In addition, the following guidance shown in [Table 21](#) for cloud services also apply.

- a) Guidance for cloud services

Table 21 — Guidance for independent review of information security

CSC	CSP
The CSC should request documented evidence that the implementation of information security controls and guidelines for the cloud service is in line with any claims made by the CSP. Such evidence can include assessment reports or certifications produced by third-party conformity assessment bodies.	The CSP should provide documented evidence to the CSC to substantiate its claim of implementing information security controls. Where individual CSC audits are impractical or can increase risks to information security, the CSP should provide independent evidence that information security is implemented and operated in accordance with the CSP's topic-specific policies and procedures. This should be made available to prospective CSCs prior to entering a contract. A relevant independent audit as selected by the CSP should be an acceptable method for fulfilling the CSC's interest in reviewing the CSP's operations, provided sufficient transparency is provided. When the independent audit is impractical, the CSP should conduct a self-assessment, and disclose its process and results to the CSC.

5.36 Compliance with policies, rules and standards for information security

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.36 apply.

5.37 Documented operating procedures

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.37 apply. In addition, the following guidance shown in [Table 22](#) and other information for cloud services also apply.

a) Guidance for cloud services

Table 22 — Guidance for documented operating procedures

CSC	CSP
The CSC should document procedures for critical operations where a failure can cause unrecoverable damage to assets in the cloud computing environment. Examples of the critical operations are: — installation, changes, and deletion of virtualized resources such as servers, networks and storage; — cryptographic key and certificate management; — termination of cloud service usage; — backup and restoration. The documents should specify what critical operations are monitored.	The CSP should provide documentation about the critical operating procedures to CSCs who require it. Examples of the critical operations are: — installation, changes, and deletion of virtualized resources such as servers, networks and storage; — cryptographic key and certificate management; — termination of cloud service usage; — backup and restoration.

b) Other information for cloud services

Cloud computing has the benefit of rapid provisioning and administration, and on-demand self-service. These operations are often carried out by administrators from the CSC and the CSP. Since human intervention in these critical operations can cause serious information security incidents, mechanisms to safeguard the operations should be considered and, if needed, be defined and implemented. Examples of serious incidents include erasing or shutting down a large number of virtual servers or destroying virtual assets.

5.38 CLD - Shared roles and responsibilities within a cloud computing environment

The following apply:

- attributes shown in [Table 23](#);
- control, purpose and guidance shown in [Table 24](#);
- other information for cloud services.

Table 23 — CLD - Shared roles and responsibilities within a cloud computing environment

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance #Supplier_relationships_security	#Governance_and_Ecosystem #Protection #Resilience

a) Control

Responsibilities for shared information security roles in the use of the cloud service should be allocated to identified parties, documented, communicated and implemented by both the CSC and the CSP.

b) Purpose

To clarify the relationship regarding shared roles and responsibilities between the CSC and the CSP for information security management.

c) Guidance for cloud services

Table 24 — Guidance for CLD – Shared roles and responsibilities within a cloud computing environment

CSC	CSP
The CSC should review the information security roles and responsibilities as defined by the CSP, 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. The CSC should identify and manage its relationship with the customer support function of the CSP. The CSC should request information from the CSP regarding the information security capabilities of the CSP such as authentication, cryptography, backup and logging. The CSC can use frameworks established by third parties or independent bodies to complement the CSP information on available security capabilities.	The CSP should define and document the allocation of information security roles and responsibilities that the CSC, the CSP and suppliers to the CSP are expected to implement. The CSP should establish and maintain the relationship regarding information security issues based on the allocation of information security roles and responsibilities with the CSC. The CSP should provide information to the CSC regarding the information security capabilities of the cloud service and information security measures taken by the CSP to assist the CSC to understand them clearly and adequately. In order to fulfil this purpose, the CSP can provide the information according to frameworks established by third parties or independent bodies.

d) Other information for cloud services

In cloud computing, roles and responsibilities are typically divided between the CSC and the CSP. The allocation of roles and responsibilities should take into consideration the CSC data and the CSC's applications for which the CSP is a custodian.

5.39 CLD - Agreement on the roles and responsibilities of the cloud service partner

The following apply:

- attributes shown in [Table 25](#);
- control, purpose, and guidance shown in [Table 26](#);

— other information for cloud services.

Table 25 — Attributes for CLD – Agreement on the roles and responsibilities of the cloud service partner

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance #Supplier_relationships_security	#Governance_and_Ecosystem #Protection #Resilience

a) Control

Information security roles and responsibilities of the CSN should be defined and agreed with the CSC or CSP that uses the CSN's service.

b) Purpose

To delineate the roles and responsibilities of the CSC and the CSP when using a CSN.

c) Guidance for cloud services

Table 26 — Guidance for CLD – Agreement on the roles and responsibilities of the cloud service partner

CSC	CSP
The CSC and the CSP using a CSN should clearly define and agree with the CSN on the roles and responsibilities to be assumed by the CSN. The CSC and the CSP have shared roles and responsibilities between them (5.38). When the CSC or the CSP has an agreement with the CSN, the agreement should be consistent with the shared roles and responsibilities between the CSC and the CSP.	

d) Other information for cloud services

The CSN role is a set of activities that support, or are auxiliary to, either the CSP role or the CSC role, or both. Activities of a CSN role vary depending on the type of partner and their relationship with the CSP role and the CSC role.

The following three sub-roles of CSN are defined in ISO/IEC 22123-3:

- cloud service developer;
- cloud auditor;
- cloud service broker.

A wide variety of cloud services are available, and CSCs can use CSNs to select the best combination of services. In this case, it is necessary to conclude an appropriate contract with CSNs regarding information security.

In some cases, the CSN can be a stand-alone role as a CSN, but in other cases, the CSN can also play a role as a CSP.

6 Cloud service specific guidance related to people controls

6.1 Screening

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 6.1 apply.

6.2 Terms and conditions of employment

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 6.2 apply.

6.3 Information security awareness, education and training

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 6.3 apply. In addition, the following guidance shown in [Table 27](#) also applies.

a) Guidance for cloud services

Table 27 — Guidance for information security awareness, education and training

CSC	CSP
Information security awareness, education and training programmes about cloud services should be provided to the stakeholders. It should cover management, the supervising managers, those of business units, cloud service administrators, cloud service integrators and CSUs, including relevant personnel and interested parties. This supports effective coordination of information security activities. These information security awareness, education and training programmes should include the following: — standards, topic-specific policies and procedures for the use of cloud services; — information security risks relating to the use of the cloud services and how those risks are managed; — system and network environment risks with the use of cloud services; — applicable legal and regulatory requirements.	The CSP should provide awareness, education and training for personnel, and require relevant interested parties to do the same, concerning the appropriate handling of CSC data and cloud service derived data. This data can contain information confidential to a CSC or be subject to specific limitations, including regulatory restrictions, on access and use by the CSP.

6.4 Disciplinary process

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 6.4 apply.

6.5 Responsibilities after termination or change of employment

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 6.5 apply.

6.6 Confidentiality or non-disclosure agreements

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 6.6 apply.

6.7 Remote working

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 6.7 apply.

6.8 Information security event reporting

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 6.8 apply. In addition, the following guidance shown in [Table 28](#) also applies.

a) Guidance for cloud services

Table 28 — Guidance for information security event reporting

CSC	CSP
The CSC should request information from the CSP about the mechanisms for: — the CSC to report an information security event it has detected to the CSP; — the CSP to report an information security event it has detected to the CSC; — the CSC to track the status of a reported information security event.	The CSP should provide mechanisms for: — the CSC to report an information security event to the CSP; — the CSP to report an information security event to the CSC; — the CSC to track the status of a reported information security event.

7 Cloud service specific guidance related to physical controls

7.1 Physical security perimeters

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 7.1 apply.

7.2 Physical entry

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 7.2 apply.

7.3 Securing offices, rooms and facilities

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 7.3 apply.

7.4 Physical security monitoring

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 7.4 apply.

7.5 Protecting against physical and environmental threats

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 7.5 apply.

7.6 Working in secure areas

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 7.6 apply.

7.7 Clear desk and clear screen

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 7.7 apply.

7.8 Equipment siting and protection

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 7.8 apply.

7.9 Security of assets off-premises

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 7.9 apply.

7.10 Storage media

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 7.10 apply.

7.11 Supporting utilities

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 7.11 apply.

7.12 Cabling security

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 7.12 apply.

7.13 Equipment maintenance

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 7.13 apply.

7.14 Secure disposal or re-use of equipment

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 7.14 apply. In addition, the following guidance shown in [Table 28](#) and other information also apply.

a) Guidance for cloud services

Table 29 — Guidance for secure disposal or re-use of equipment

CSC	CSP
The CSC should request information about the process and methods for the secure disposal or reuse of resources (e.g. equipment, data storage, files, memory).	The CSP should provide the CSC with information about the process and methods for the secure disposal or re-use of resources (e.g. equipment, data storage, files, memory).

b) Other information for cloud services

Sound record-keeping and change management practices support traceability and auditability, as well as preventing inappropriate disposal or re-use of equipment. Additional information about secure disposal can be found in ISO/IEC 27040.

8 Cloud service specific guidance related to technological controls

8.1 User endpoint devices

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.1 apply.

8.2 Privileged access rights

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.2 apply. In addition, the following guidance shown in [Table 30](#) also applies.

a) Guidance for cloud services

Table 30 — Guidance for privileged access rights

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

8.3 Information access restriction

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.3 apply. In addition, the following guidance shown in [Table 31](#) and other information for cloud services also apply.

a) Guidance for cloud services

Table 31 — Guidance for information access restriction

CSC	CSP
The CSC should ensure that access to information in the cloud service can be restricted according to its topic-specific policy on access control and that such restrictions are implemented. This includes restricting access to: — the cloud services; — the cloud service functions of the cloud services; — the CSC data maintained in the cloud service.	The CSP should provide the capabilities and information regarding access controls that allow the CSC to restrict access to: — the cloud services; — the cloud service functions of the cloud services; — the CSC data maintained in the cloud service.

b) 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, should have additional access control. Both the CSC and the CSP can have responsibilities to these additional areas for access controls.

An architecture based on “zero trust” principles can be used for controlling access to distributed resources in a multi-cloud environment. Additional information about “zero trust” principles can be found in ISO/IEC 27002:2022, 8.27.

8.4 Access to source code

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.4 apply.

8.5 Secure authentication

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.5 apply.

8.6 Capacity management

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.6 apply. In addition, the following guidance shown in [Table 32](#) and other information for cloud services also apply.

a) Guidance for cloud services

Table 32 — Guidance for capacity management

CSC	CSP
The CSC should ensure that the capacity provided by the CSP meets the CSC's requirements. The CSC should monitor the resource usage in the cloud services, and forecast the capacity needs, to ensure performance of the cloud services over time. The CSC should have access to relevant data on: — the resource usage for particular time periods; — the maximum levels of resource usage. The CSC should notify the CSP of additional capacity requirements when the CSP provides a process for responding to such requests. Failure to do so can result in unexpected stockouts.	The CSP should provide the CSC with data for monitoring its resource usage through tools or APIs for monitoring the CSC's resource usage. The CSP should provide a process for responding to additional capacity requirements.

b) Other information for cloud services

Cloud services involve resources that are under the control of the CSP and made available to the CSC under the terms of the cloud 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 resources assigned to the CSC can 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 CSC purchases. If the CSC has requirements that exceed the constraints, it can be necessary for the CSC to change the cloud service or change the subscription.

8.7 Protection against malware

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.7 apply.

8.8 Management of technical vulnerabilities

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.8 apply. In addition, the following guidance shown in [Table 33](#) also applies.

a) Guidance for cloud services

Table 33 — Guidance for management of technical vulnerabilities

CSC	CSP
The CSC should request information from the CSP about the management of technical vulnerabilities that can affect the cloud services provided. The CSC should define its process for managing these technical vulnerabilities. The CSC should determine which technical vulnerabilities are expected to be addressed.	The CSP should make available to the CSC information about the management of technical vulnerabilities that can affect the cloud services provided.

8.9 Configuration management

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.9 apply. In addition, the following guidance shown in [Table 34](#) and other information for cloud services also apply.

a) Guidance for cloud services

Table 34 — Guidance for configuration management

CSC	CSP
The CSC should define the responsibilities regarding configuration management for the use of the cloud service. The CSC should define and implement configuration management processes and tools for the cloud service considering: — availability of documented information for the secure configuration of the cloud service; — availability of configuration management capabilities provided by the CSP; — ability to continuously monitor whether the provided standard templates satisfy the topic-specific policy on configuration management and requirement of the CSC; — ability to customize the standard templates provided by the CSP to reflect its topic-specific policy on configuration management or target security posture, which can be in different formats.	The CSP should provide information to the CSC about the CSC's configuration management responsibilities. The CSP should provide: — information on the secure configuration for the use of the cloud service; — functions and tools supporting the configuration management of the CSC; — standard templates of the cloud service.

b) Other information for cloud services

When configuring virtual environments, the CSC and the CSP should ensure that appropriate aspects are hardened (e.g. eliminating unnecessary support for or access to protocols, network ports, services, applications, utility programs, portals, APIs, and the use of fine-grained cloud service configuration to enhance identity and access restrictions).

For more information on the monitoring of cloud services for the purpose of configuration management, see [Annex B](#).

8.10 Information deletion

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.10 apply. In addition, the following guidance shown in [Table 35](#) and other information for cloud services also apply.

a) Guidance for cloud services

Table 35 — Guidance for information deletion

CSC	CSP
The CSC should request a documented description of the process of termination of the agreement for the use of the service that covers removal of CSC's assets followed by the deletion of all copies of those assets from the CSP's systems. The description should list all the assets including CSC data and cloud service derived data. The description should also document the scheduled termination of the agreement to use the service, which should occur in a timely manner.	The CSP should provide information about the arrangements for the removal of any CSC's assets upon termination of the cloud service agreement. The asset removal arrangements should be documented in the agreement and should be performed in a timely manner. The arrangements should specify the assets to be removed or kept, including CSC data and cloud service derived data, and document the scheduled termination of the agreed service.

b) Other information for cloud services

See also [5.11](#) for the case where the return of assets of the CSC is required.

8.11 Data masking

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.11 apply. In addition, the following guidance shown in [Table 36](#) also applies.

a) Guidance for cloud services

Table 36 — Guidance for data masking

CSC	CSP
If data masking is required, the CSC should confirm if it can be performed using the cloud service in compliance with the CSC's topic-specific policies on data masking. If the data masking function provided by the cloud service does not meet the needs of the topic-specific policy on data masking, the CSC should implement its own data masking.	When the CSP delivers data masking capability of the cloud service for the CSC, the CSP should provide information about such capabilities.

8.12 Data leakage prevention

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.12 apply.

8.13 Information backup

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.13 apply. In addition, the following guidance shown in [Table 37](#) and other information for cloud services also apply.

a) Guidance for cloud services

Table 37 — Guidance for information backup

CSC	CSP
Where the CSP provides backup capability as part of the cloud service, the CSC should request its specifications. The CSC should verify that the backup capability meets the CSC's backup requirements. The CSC is responsible for implementing backup capabilities, when the backup capabilities provided by the CSP do not meet the CSC's requirements.	The CSP should provide the specifications of its backup capabilities to the CSC. The specifications should include the following information, as appropriate: — scope and schedule of backups; — backup methods and data formats, including encryption, if relevant; — retention periods for backup data; — procedures for verifying integrity of backup data; — procedures and timescales involved in restoring data from backup; — procedures to test the backup capabilities; — storage location of backups. If the backup function is provided to the CSC, it should have secure access control to maintain confidentiality and integrity of the backups.

b) 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 CSC. However, it is possible that a CSC is not aware of its responsibility to make backups of all CSC 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 capabilities can be offered as a service at additional cost and, in this case, CSCs can choose what and when to backup.

8.14 Redundancy of information processing facilities

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.14 apply.

8.15 Logging

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.15 apply. In addition, the following guidance shown in [Table 38](#) and other information for cloud services also apply.

a) Guidance for cloud services

Table 38 — Guidance for logging

CSC	CSP
The CSC should define its requirements for logging and verify that the cloud service meets those requirements or the CSC should implement additional logging capabilities. If a privileged operation is delegated to the CSC, the operation and performance of those operations should be logged by the capabilities provided by the CSP or by additional logging capabilities implemented by the CSC.	The CSP should provide capabilities and information regarding logging to the CSC.

b) Other information for cloud services

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

8.16 Monitoring activities

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.16 apply. In addition, the following guidance shown in [Table 39](#) and other information for cloud services also apply.

a) Guidance for cloud services

Table 39 — Guidance for monitoring activities

CSC	CSP
The CSC should request information from the CSP of the service monitoring capabilities related to information security available for each cloud service. The CSC can use the tools for monitoring provided by the CSP or third-party vendors.	The CSP should provide capabilities and a description that enable the CSC to monitor specific information security aspects, relevant to the CSC, of the operation of the cloud service. These capabilities can include monitoring to detect if the cloud service is being used as a platform to attack others, or if traffic data show abnormal behaviour. Appropriate access controls should secure the use of the monitoring capabilities. The capabilities should provide access only to information about the CSC's own cloud service instances. Monitoring should provide data consistent with the logs described in 8.15 and assist with cloud SLA terms.

b) Other information for cloud services

For more information on the monitoring of cloud services, see [Annex B](#).

The ISO/IEC 19086 series provides information on cloud SLAs.

8.17 Clock synchronization

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.17 apply. In addition, the following guidance shown in [Table 40](#) and other information for cloud services also apply.

a) Guidance for cloud services

Table 40 — Guidance for clock synchronization

CSC	CSP
The CSC should request information about the clock synchronization for the CSP's systems.	The CSP should provide information to the CSC regarding the clock synchronization by the CSP's systems, and information about how the CSC can synchronise local clocks with the cloud service clock.

b) Other information for cloud services

When using cloud services, it is necessary to consider the synchronisation of the CSC's systems with the CSP's systems that are running the cloud services used by the CSC. Without such synchronisation, it can be difficult to reconcile events on the CSC's systems with events on the CSP's systems.

8.18 Use of privileged utility programs

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.18 apply. In addition, the following guidance shown in [Table 41](#) and other information for cloud services also apply.

a) Guidance for cloud services

Table 41 — Guidance for use of privileged utility programs

CSC	CSP
The CSC should identify the utility programs expected to be used in its cloud computing environment and ensure that they do not interfere with the controls of the cloud service.	The CSP should identify the requirements for any utility programs which the CSC is authorized to operate in the CSP's environment. When a utility program is provided as part of the cloud service, the CSP should ensure it is adequately secure.

b) Other information for cloud services

In cloud services, it is possible for the CSC's personnel to change settings for the entire tenant or to create, modify or delete resources by using command line tools or APIs provided by the CSP. Only authorized personnel should be permitted to use these tools with appropriate access provided. Access to such tools should be managed by authentication and authorization controls.

8.19 Installation of software on operational systems

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.19 apply.

8.20 Network security

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.20 apply. In addition, the following guidance shown in [Table 42](#) and other information for cloud services also apply.

a) Guidance for cloud services

Table 42 — Guidance for network security

CSC	CSP
(no additional guidance)	The CSP should define and document a topic-specific policy on the configuration of the virtual network consistent with the topic-specific policy for the physical network. The CSP should ensure that the virtual network configuration matches the topic-specific policy on configuration of the virtual network, regardless of the means used to create the configuration.

b) Other information for cloud services

In a cloud computing environment built on virtualization technology, a virtual network is configured on virtual infrastructure on a physical network. In such environments, inconsistency of topic-specific policies on networks can cause system outages or defective access control.

NOTE Depending on the type of the cloud service, the responsibilities for configuring a virtual network can vary between a CSC and a CSP.

8.21 Security of network services

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.21 apply.

8.22 Segregation of networks

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.22 apply.

8.23 Web filtering

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.23 apply.

8.24 Use of cryptography

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.24 apply. In addition, the following guidance shown in [Table 43](#) also applies.

a) Guidance for cloud services

Table 43 — Guidance for use of cryptography

CSC	CSP
When the CSP offers cryptography, the CSC should review any information supplied by the CSP to confirm whether the cryptographic capabilities: — meet the CSC's information security requirements of cryptography; — are compatible with any other cryptographic protection used by the CSC; — apply to data at rest and in transit to, from and within the cloud service. Where the CSP provides key management functionality for use by the CSC, the CSC should request the following information on the procedures used to manage keys related to the cloud service: — type of keys; — specifications of the key management system, including procedures for each stage of the key life-cycle (e.g. generating, changing or updating, storing, retiring, retrieving, retaining and destroying); — recommended key management procedures for use by the CSC. In certain cases, it can be necessary for the CSC to take on the burden of operating its own key management applied to some part of its assets. In these cases, the CSC should review the constraints and tooling made available by the CSP, and employ or build the appropriate cryptographic tooling.	The CSP should provide information to the CSC regarding the circumstances in which it uses cryptography to protect the information it processes. The CSP should provide information to the CSC regarding the procedures to manage keys related to the cloud service. The CSP should also provide information to the CSC about any capabilities it provides that can assist the CSC in applying its own cryptographic protection.

8.25 Secure development life cycle

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.25 apply. In addition, the following guidance shown in [Table 44](#) and other information for cloud services also apply.

a) Guidance for cloud services

Table 44 — Guidance for secure development life cycle

CSC	CSP
The CSC should request information from the CSP about the CSP's use of secure development procedures and practices.	The CSP should provide information about its use of secure development procedures and practices to the extent compatible with its policy for disclosure.

b) Other information for cloud services

Secure development procedures and practices of the CSP can be critical to SaaS.

8.26 Application security requirements

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.26 apply.

8.27 Secure system architecture and engineering principles

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.27 apply.

8.28 Secure coding

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.28 apply.

8.29 Security testing in development and acceptance

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.29 apply.

a) Other information for cloud services

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

8.30 Outsourced development

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.30 apply.

8.31 Separation of development, test and production environments

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.31 apply.

8.32 Change management

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.32 apply. In addition, the following guidance shown in [Table 45](#) and other information for cloud services also apply.

a) Guidance for cloud services

Table 45 — Guidance for change management

CSC	CSP
The CSC's change management process should take into account the impact of any changes made by the CSP in correlation with changes made by the CSC.	The CSP should provide the CSC with information regarding changes to the cloud service that can adversely affect the cloud service. The CSP can consider the following to support CSC determining the impact of a proposed change on information security: — categories of changes; — planned date and time of the changes; — technical description of the changes to the cloud service and underlying systems; — notification of the start and the completion of the changes. When the CSP offers a cloud service that depends on a secondary CSP, then it can be necessary for the CSP to inform the CSC of changes caused by the secondary CSP.

b) 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 cloud service agreement or a cloud SLA.

The ISO/IEC 19086 series provides information on cloud SLAs.

8.33 Test information

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.33 apply.

8.34 Protection of information systems during audit and testing

The attributes, control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.34 apply.

8.35 CLD - Segregation in virtual computing environments

The following apply:

- attributes shown in [Table 46](#);
- control, purpose and guidance shown in [Table 47](#);
- other information for cloud services.

Table 46 — Attributes for CLD – Segregation in virtual computing environments

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security #Secure_configuration #Supplier_relationships_security	#Protection

a) Control

A CSC's virtual environment running on a cloud service should be protected from unauthorized access.

b) Purpose

To prevent inappropriate access or disclosure of information through insecure virtualization.

c) Guidance for cloud services

Table 47 — Guidance for CLD – segregation in virtual computing environments

CSC	CSP
The CSC should define its requirements for segregating the CSCs' environments to achieve tenant isolation in the shared virtual environment of the cloud service and verify that the CSP meets those requirements.	The CSP should enforce logical segregation of CSC data, virtualized applications, operating systems, storage, and network for the separation of resources in a multi-tenant environment to ensure isolation of resources used by different tenants. The CSP should consider the risks associated with running CSC-supplied software within the cloud services offered by the CSP. The CSP should also enforce the separation of the CSP's internal administration from resources used by CSCs.

d) Other information for cloud services

Unauthorized access which can exploit inadequate segregation of virtual computing environments can include access to the CSC's environment from third parties and other CSCs. Segregation in virtual computing environments can mitigate the risk of adversely affecting other tenants when one tenant experiences unauthorized access. Unauthorized access can include access from personnel of the CSP to the CSC's environment.

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

Implementation of logical segregation depends upon the technologies applied to the virtualization. Network and storage configurations can be virtualized when a software virtualization function provides a virtual environment (e.g. a virtual operating system or container isolation). In addition, segregation of CSCs in software virtualized environments can be designed and implemented using segregation functions of the software.

Secure multi-tenancy and related guidance given in ISO/IEC 27040 can apply to the cloud computing environment.

8.36 CLD - Detection and prevention of unauthorized use of cloud services

The following apply:

- attributes shown in [Table 48](#),
- control, purpose and guidance shown in [Table 49](#).

Table 48 — Attributes for CLD – Detection and prevention of unauthorized use of cloud services

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Protect #Detect #Respond	#System_and_network_security #Information_security_event_management #Supplier_relationships_security	#Protection #Defence

a) Control

The CSUs' use of cloud services should be monitored to prevent unauthorized access, data transfer and other activities on cloud services.

b) Purpose

To enable monitoring and prevention of unintended use of cloud services and unintended data transfer to and from cloud services.

c) Guidance for cloud services

Table 49 — Guidance for CLD - Detection and prevention of unauthorized use of cloud services

CSC	CSP
The CSC should consider implementing: — monitoring of CSUs' activities; — periodic technical compliance review with the information security policy, topic-specific policy on the use of cloud services and relevant rules and standards; — monitoring and prevention of unintended or unauthorized information transfer to and from the cloud service environment managed by the CSC; — detection of anomalies, such as increasing resource utilization and unknown service usage by detecting deviations from normal conditions.	The CSP should provide the CSC with guidance and functions to monitor and control the CSUs' use of the cloud service.

Annex A (Informative)

Correspondence between this document and the first edition (ISO/IEC 27017:2015)

The purpose of this annex is to provide the mappings between the set of controls of this document and the previous edition (ISO/IEC 27017:2015) for organizations currently using it and wanting to transition to this edition.

[Table A.1](#) lists:

- in the left columns, the controls from this document;
- in the right columns, the controls inherited from ISO/IEC 27017:2015.

The mappings of controls between this document and ISO/IEC 27017:2015 that are not specific to cloud services are omitted because they are covered by ISO/IEC 27002:2022, Table B.1.

Table A.1 — Correspondence between controls in this document and ISO/IEC 27017:2015

ISO/IEC 27017:2026			ISO/IEC 27017:2015		
Control identifier	Control name	Control statement	Control identifier	Control name	Control statement
5.11	Return of assets	Personnel and other interested parties as appropriate should return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.	8.1.4	Return of assets	All employees and external party users should return all of the organizational assets in their possession upon termination of their employment, contract or agreement.
			CLD.8.1.5	Removal of cloud service customer assets	Assets of the cloud service customer that are on the cloud service provider's premises should be removed, and returned if necessary, in a timely manner upon termination of the cloud service agreement.
5.37	Documented operating procedures	Operating procedures for information processing facilities should be documented and made available to personnel who need them.	12.1.1	Documented operation procedures	Operating procedures should be documented and made available to all users who need them.
			CLD.12.1.5	Administrator's operational security	Procedures for administrative operations of a cloud computing environment should be defined, documented and monitored.

Table A.1 (continued)

ISO/IEC 27017:2026			ISO/IEC 27017:2015		
Control identifier	Control name	Control statement	Control identifier	Control name	Control statement
5.38	CLD - Shared roles and responsibilities within a cloud computing environment	Responsibilities for shared information security roles in the use of the cloud service should be allocated to identified parties, documented, communicated and implemented by both the CSC and the CSP.	CLD.6.3.1	Shared roles and responsibilities within a cloud computing environment	Responsibilities for shared information security roles in the use of the cloud service should be allocated to identified parties, documented, communicated and implemented by both the cloud service customer and the cloud service provider.
5.39^a	CLD - Agreement on the roles and responsibilities of the cloud service partner	Information security roles and responsibilities of the CSN should be defined and agreed with the CSC or CSP that uses the CSN's service.	No corresponding control in ISO/IEC 27017:2015		
8.9^b	Configuration management	Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed.	No corresponding control in ISO/IEC 27017:2015		
			CLD.9.5.2	Virtual machine hardening	Virtual machines in a cloud computing environment should be hardened to meet business needs.
8.10^b	Information deletion	Information stored in information systems, devices or in any other storage media should be deleted when no longer required.	No corresponding control in ISO/IEC 27017:2015		
			CLD.8.1.5	Removal of cloud service customer assets	Assets of the cloud service customer that are on the cloud service provider's premises should be removed, and returned if necessary, in a timely manner upon termination of the cloud service agreement.
8.16^b	Monitoring activities	Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	No corresponding control in ISO/IEC 27017:2015		
			CLD.12.4.5	Monitoring of Cloud Services	The cloud service customer should have the capability to monitor specified aspects of the operation of the cloud services that the cloud service customer uses.

Table A.1 (continued)

ISO/IEC 27017:2026			ISO/IEC 27017:2015		
Control identifier	Control name	Control statement	Control identifier	Control name	Control statement
8.20	Network security	Networks and network devices should be secured, managed and controlled to protect information in systems and applications.	13.1.1	Network security	Networks should be managed and controlled to protect information in systems and applications.
			CLD.13.1.4	Alignment of security management for virtual and physical networks	Upon configuration of virtual networks, consistency of configurations between virtual and physical networks should be verified based on the cloud service provider's network security policy.
8.35	CLD -Segregation in virtual computing environments	A CSC's virtual environment running on a cloud service should be protected from unauthorized access.	CLD.9.5.1	Segregation in virtual computing environments	A cloud service customer's virtual environment running on a cloud service should be protected from other cloud service customers and unauthorized persons.
8.36 ^a	CLD - Detection and prevention of unauthorized use of cloud services	The CSUs' use of cloud services should be monitored to prevent unauthorized access, data transfer and other activities on cloud services.	No corresponding control in ISO/IEC 27017:2015		
^a New control in this document.					
^b New control in ISO/IEC 27002:2022.					

[Table A.2](#) lists:

- in the left columns, the controls from ISO/IEC 27017:2015;
- in the right columns, the controls from this document, which inherit the controls from the previous edition.

The mappings of controls between ISO/IEC 27017:2015 and this document that are not specific to cloud services are omitted because they are covered by ISO/IEC 27002:2022, Table B.2.

Table A.2 — Correspondence between controls in ISO/IEC 27017:2015 and this document

ISO/IEC 27017:2015			ISO/IEC 27017:2026		
Control identifier	Control name	Control statement	Control identifier	Control name	Control statement
CLD.6.3.1	Shared roles and responsibilities within a cloud computing environment	Responsibilities for shared information security roles in the use of the cloud service should be allocated to identified parties, documented, communicated and implemented by both the cloud service customer and the cloud service provider.	5.38	CLD - Shared roles and responsibilities within a cloud computing environment	Responsibilities for shared information security roles in the use of the cloud service should be allocated to identified parties, documented, communicated and implemented by both the CSC and the CSP.
CLD.8.1.5	Removal of cloud service customer assets	Assets of the cloud service customer that are on the cloud service provider's premises should be removed, and returned if necessary, in a timely manner upon termination of the cloud service agreement.	5.11	Return of assets	Personnel and other interested parties as appropriate should return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.
			8.10^a	Information deletion	Information stored in information systems, devices or in any other storage media should be deleted when no longer required.
CLD.9.5.1	Segregation in virtual computing environments	A cloud service customer's virtual environment running on a cloud service should be protected from other cloud service customers and unauthorized persons.	8.35	CLD - Segregation in virtual computing environments	A CSC's virtual environment running on a cloud service should be protected from unauthorized access.
CLD.9.5.2	Virtual machine hardening	Virtual machines in a cloud computing environment should be hardened to meet business needs.	8.9^a	Configuration management	Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed.
CLD.12.1.5	Administrator's operational security	Procedures for administrative operations of a cloud computing environment should be defined, documented and monitored.	5.37	Documented operating procedures	Operating procedures for information processing facilities should be documented and made available to personnel who need them.

Table A.2 (continued)

ISO/IEC 27017:2015			ISO/IEC 27017:2026		
Control identifier	Control name	Control statement	Control identifier	Control name	Control statement
CLD.12.4.5	Monitoring of Cloud Services	The cloud service customer should have the capability to monitor specified aspects of the operation of the cloud services that the cloud service customer uses.	8.16^a	Monitoring activities	Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.
CLD.13.1.4	Alignment of security management for virtual and physical networks	Upon configuration of virtual networks, consistency of configurations between virtual and physical networks should be verified based on the cloud service provider's network security policy.	8.20	Network security	Networks and network devices should be secured, managed and controlled to protect information in systems and applications.
^a New control in ISO/IEC 27002:2022					

Annex B (informative)

Monitoring of cloud services

Cloud computing introduces changes in the way that monitoring activities (see [8.16](#)) and configuration management (see [8.9](#)) are conducted. In traditional computing, those monitoring activities involved installing agents on specific equipment, and collecting, reviewing and evaluating logs for sources of potential issues. These tasks can be performed manually or automatically through software tools. Although these tasks can be performed through a third party (e.g. IT services supplier), the same process is followed.

In cloud computing, there is a specific degree of transparency of the systems and a specific degree of monitoring that can be performed by the CSC. Depending on the service model, the degree can range from insubstantial (SaaS) to increased (IaaS). The CSC and the CSP have specific roles and responsibilities regarding monitoring, either for the detection of security-relevant events or for configuration management purposes. For example, when a CSC uses SaaS, the security monitoring functions that can be implemented by the CSC are limited to those related to software usage. In the case of an IaaS, the CSC can leverage tools provided by CSPs that have a broader range of functions for continuous monitoring. Such tools can have a function of monitoring the standard configuration templates offered by the CSP if they conform to the CSC's information security policy. In both examples, the CSC has no monitoring capabilities on the logical and physical infrastructure that supports the provision of the cloud service. In these cases, the CSC (depending also on the agreed upon terms of service) is expected to be satisfied with the information shared by the CSP (see [5.38](#)).

Monitoring of the cloud service for configuration management purposes is expected to rely on "automated monitoring" or "monitoring with automation" (e.g. gathering and pre-processing data by non-human means). The introduction of automated monitoring for configuration management activities can leverage available technologies (e.g. Cloud Security Posture Management) and machine-readable languages [e.g. Open Security Controls Assessment Language (OSCAL)] in managing the complexity and scale of cloud services.

"Automated monitoring" can facilitate processes and practices of auditing cloud services. Auditing is a systematic, independent and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which:

- the audit criteria are fulfilled;
- the available information is limited;
- relevant risk treatment options are adapted and supported with available tools.

For the mentioned SaaS example above and for the criterion related to access control, an auditor is expected to collect and evaluate evidence for the access control within the SaaS application. For the other cases, the collected evidence can be just the relevant agreements of the cloud service.

Different service models introduce differences in the allocation of responsibilities and required abilities for monitoring and auditing between the CSC and the CSP. Generally, SaaS often offers the most limited auditing and monitoring capabilities for the CSC while providing the most extensive capabilities for the CSPs.

In conclusion, for the CSC, within the project of cloud computing transition, monitoring and configuration management should be implemented and supported by automated monitoring. For the CSP, on the other hand, monitoring and configuration management should cover their own needs for the effective and efficient operation of the relevant services as well as making provisions for the information needs of the CSC.

Bibliography

- [1] ISO/IEC 5140, *Information technology — Cloud computing — Concepts for multi-cloud and the use of multiple cloud services*
- [2] ISO/IEC 19086 (all parts), *Cloud computing — Service level agreement (SLA) framework*
- [3] ISO 19440:2020, *Enterprise modelling and architecture — Constructs for enterprise modelling*
- [4] ISO/IEC 22123-3:2023, *Information technology — Cloud computing — Part 3: Reference architecture*
- [5] ISO/IEC 27001, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*
- [6] ISO/IEC 27005, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*
- [7] ISO/IEC 27017:2015²⁾, *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*
- [8] ISO/IEC 27018, *Information security, cybersecurity and privacy protection — Guidelines for protection of personally identifiable information (PII) in public clouds acting as PII processors*
- [9] ISO/IEC 27036-1:2021, *Cybersecurity — Supplier relationships — Part 1: Overview and concepts*
- [10] ISO/IEC 27036-2:2022, *Cybersecurity — Supplier relationships — Part 2: Requirements*
- [11] ISO/IEC 27036-3:2023, *Cybersecurity — Supplier relationships — Part 3: Guidelines for hardware, software, and services supply chain security*
- [12] ISO/IEC 27036-4:2016, *Information technology — Security techniques — Information security for supplier relationships — Part 4: Guidelines for security of cloud services*
- [13] ISO/IEC 27040, *Information technology — Security techniques — Storage security*
- [14] ISO 31000, *Risk management — Guidelines*

2) Cancelled and replaced by this document (ISO/IEC 27017:2026).



ICS 03.100.70; 35.030

Price based on 39 pages

© ISO/IEC 2026
All rights reserved

iso.org