ISO/IEC JTC 1/SC 27 "Information security, cybersecurity and privacy protection"
Secretariat: **DIN**
Committee manager: **Mahmoud Sobhi Mr**

ISO/IEC CD 27017

Document type	Related content	Document date	Expected action
Ballot / Reference document	Ballot: ISO/IEC CD 27017 (restricted access)	2023-10-23	**COMMENT/REPLY** by 2023-12-19

ISO/IEC JTC 1/SC 27/WG 1 "Information security management systems"
Convenorship: **BSI**
Convenor: **Humphreys Edward Prof.**

CD text for ISO/IEC 27017 (revision)

Document type	Related content	Document date	Expected action
Project / Other		2023-10-18	

ISO/IEC 27017:####(E)

ISO SC 27/WG 1

Date: 2023-10-17

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

CD stage

Warning for WDs and CDs

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Contents

Foreword

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating, and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a world-wide basis. The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups that, in turn, produce Recommendations on these topics. The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1. In some areas of information technology that fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes 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 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. ISO 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.

This document was prepared by Technical Committee ISO/IEC JTC 1 Information technology, Subcommittee SC 27, Information security, cybersecurity and privacy protection, in collaboration with ITU-T. The identical text is published as ITU-T Recommendation X.1631.

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

The main changes are as follows:

— the title has 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. The complete correspondence can be found in Annex B.

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.

Introduction

The guidelines contained within this Recommendation | International Standard are in addition to and complement the guidelines given in ISO/IEC 27002:2022.

Specifically, this Recommendation | International Standard provides guidelines supporting the implementation of information security controls for cloud service customers and cloud service providers. Some guidelines are for cloud service customers who implement the controls and others are for cloud service providers to support the implementation of those controls. The determination of the appropriate information security controls and the extent of the utilisation of the guidance provided will depend 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 Recommendation | International Standard gives guidelines for information security controls applicable to the provision and use of cloud services by providing:

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

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

This Recommendation | International Standard excludes any and all aspects of conformity assessment.

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 27000, *Information technology — Security techniques — Information security management systems — Overview and 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 27000, 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

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 Cloud computing specific concepts

4.1 General

4.1.1 Overview

This Recommendation | International Standard provides additional cloud-specific guidance based on ISO/IEC 27002 and provides additional controls to address cloud-specific information security threats and risks considerations.

Users of this Recommendation | International Standard should refer to Clauses 5 to 8 in ISO/IEC 27002:2022 for controls, purposes, guidance and other information. Because of 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, "5.3 Segregation of duties" of ISO/IEC 27002 provides a control that can be applied whether the organization is acting as a cloud service provider or not. Additionally, a cloud service customer can derive requirements for segregation of duties in the cloud environment from the same control, e.g., a cloud service customer segregating the cloud service customers' cloud service administrators from other cloud service users.

As an extension to ISO/IEC 27002:2022, this Recommendation | International Standard further provides cloud service specific controls, purposes, guidance and other information that are intended to mitigate the risks that accompany the technical and operational features of cloud services (see clause 4.1.2 for the structure of this document). Annex B provides a mapping for backwards compatibility with ISO/IEC 27017:2015. The cloud service customers and the cloud service providers can refer to ISO/IEC 27002:2022 and this Recommendation | International Standard to determine controls with the guidance and add other controls if necessary. This process can be done by performing an information security risk assessment and risk treatment in the organizational and business context where cloud services are used or provided (see clause 4.2.3).

NOTE This Recommendation | International Standard is applicable to all different cloud deployment models including the private cloud. Even in this case, the controls and guidance of this document could be applicable, although adjustments would be needed to adjust to the relationships and abilities of the internal departments of an organization.

4.1.2 Structure of this International Standard

This Recommendation | International Standard is structured in a format similar to ISO/IEC 27002:2022.

This Recommendation | International Standard 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 are 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 cloud service customers and the cloud service provider without a need for any additional information, only a reference to ISO/IEC 27002:2022 is provided.

When a control is needed in addition to those of ISO/IEC 27002, cloud service extended controls are given in Annex A accompanied by the “CLD” (CLouD service extended controls)” prefix. When a control of ISO/IEC 27002:2022 or Annex A needs additional cloud service specific guidance related to the control, it is given under the subtitle “guidance for cloud services”. The guidance is provided in one of the following two types:

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

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

Type 1

Cloud service customer	Cloud service provider

Type 2

Cloud service customer	Cloud service provider

4.2 Cloud computing specific concepts

4.2.1 Supplier relationships in cloud services

Subclauses 5.19 to 5.22 of ISO/IEC 27002:2022 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 a kind of supplier relationship, where the cloud service customer is an acquirer, and the cloud service provider is a supplier. Therefore, the clause applies to cloud service customers and cloud service providers.

Cloud service customers and cloud service providers can also form a supply chain. Suppose that a cloud service provider provides a cloud service of infrastructure capabilities type. On top of this service, another cloud service provider can provide a cloud service of application capabilities type. In this case, the second cloud service provider is a cloud service customer with respect to the first, and a cloud service provider with respect to the cloud service customer using its service. In this scenario, the organization has both cloud service customer and cloud service provider roles. Every cloud service customer needs to consider which controls are applicable to it in its role as the cloud service provider and the cloud service customer. This example illustrates the case where this Recommendation | International Standard applies to an organization both as a cloud service customer and as a cloud service provider. Because cloud service customers and cloud service providers form a supply chain through the provision and use of the cloud service(s), "5.21 Managing information security in the ICT supply chain" of ISO/IEC 27002:2022 applies.

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

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

4.2.2 Relationships between cloud service customers and cloud service providers

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

Before entering into a supplier relationship, the cloud service customer needs to select a cloud service, taking into account the possible gaps between the cloud service customer's information security requirements and the information security capabilities offered by the service. Once a cloud service is selected, the cloud service customer should manage the use of the cloud service in such a way as to meet its information security requirements. In this relationship, the cloud service provider should provide the information and technical support that are necessary to meet the cloud service customer's information security requirements. When the information security controls provided by the cloud service provider

are pre-set and cannot be changed by the cloud service customer, the cloud service customer may need to implement additional controls of its own to mitigate risks.

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

— Multi-cloud, combines public cloud services from two or more cloud service providers;

— Federated cloud, combines resources from members of a cloud service federation to provide cloud services;

— Hybrid cloud, combines a private cloud with a public cloud;

— Hybrid multi-cloud, combines a hybrid cloud with a multi-cloud;

— Inter-cloud, combines the cloud services from a primary cloud service provider with one or more cloud services from secondary cloud service providers.

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

— The cloud service customer controls and manages the cloud services that are being delivered by each of the cloud service providers including their orchestration into a cloud solution (e.g. multi-cloud);

— One cloud service provider combines the cloud services from multiple cloud service providers with varying degrees of orchestration, control and management activities (e.g. inter-cloud);

— Multiple cloud service providers 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 cloud service providers resources).

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.

It is important to understand that cloud security needs collaborative effort between the cloud service provider and the cloud service customer for the provision and use of the cloud service. Cloud security is a shared responsibility between the cloud service provider and the cloud service customer. The allocation of roles and responsibilities needs to be understood and be managed. More information can be found also in CLD.5.38.

4.2.3 Managing information security risks in cloud services

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

The controls and guidance given in Clauses 5 to 8 and Annex A of this Recommendation | International Standard are used as a reference for determining and implementing controls for cloud services.

5 Cloud service specific guidance related to organizational controls

5.1 Policies for information security

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.1 and the following additional guidance apply.

Guidance for cloud services

Cloud service customer	Cloud service provider

An information security policy on the use of cloud services should be defined as a topic-specific policy of the cloud service customer. The cloud service customer'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 associate assets. When defining the information security policy on the use of cloud services, the cloud service customer should take the following into account: — information stored in the cloud computing environment can be subject to access and management by the cloud service provider; — assets can be maintained in the cloud computing environment, e.g. virtual machine instances, cloud storage buckets; — processes can run on a multi-tenant, virtualized cloud service; — access level of the cloud service users and the context in which they use of the cloud service; — the cloud service administrators of the cloud service customer who have privileged access; —the geographical locations of the cloud service provider's organization and the countries where the cloud service provider can store and process the cloud service customer data and cloud service derived data (even temporarily).	An topic-specific policy for the provision of the cloud service should be defined to support the information security policy of the cloud service provider, 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 cloud service customer isolation; — virtualization of resources including servers, containers, and networks; — access to the cloud service customer assets and cloud service derived data by the personnel of the cloud service provider; — access control procedures, e.g. strong authentication for administrative access to cloud services; — lifecycle management of cloud service customer accounts; — communications to cloud service customers during change management; — communication of breaches and information sharing guidelines to aid investigations and forensics.

Other information for cloud services

The information security policy for the use of cloud services of the cloud service customer 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 cloud service customer. 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 information security policy for provision of the cloud services deals with the cloud service customers' information and business processes, not with the cloud service provider's information and business processes. The policy should address information security in the cloud service environment and provision of functions and information supporting the cloud service customers' information security.

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

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

5.2 Information security roles and responsibilities

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.2 and the following additional guidance apply.

Guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should define information security roles and responsibilities for the use of cloud services and document them in the policies and procedures. The cloud service customer should allocate the roles and responsibilities and make relevant cloud service users aware of them.	The cloud service provider should define and allocate information security roles and responsibilities that relate to the provision of the cloud service.

Other information for cloud services

ISO/IEC 22123-3 defines roles and sub-roles of the cloud service customer and the cloud service provider.

5.3 Segregation of duties

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

5.4 Management responsibilities

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

5.5 Contact with authorities

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

Guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should identify the authorities relevant to the combined operation of the cloud service customer and the cloud service provider.	The cloud service provider should conduct a legal assessment to assess investigation requests from government agencies. The legal assessment should determine whether the government agency has an applicable and legally valid basis for the request and what additional steps need to be taken.

	The cloud service customer should inform the affected cloud service customers 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 cloud service provider should only grant access to or disclose the cloud service customer's data in the context of the government investigation request after the cloud service provider's legal assessment has shown that an applicable and valid legal basis exists. The cloud service provider should document and implement procedures to limit the cloud service customer's data access to the government agencies to only address the investigation request and not by default to all cloud service customers data.

5.6 Contact with special interest groups

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

5.7 Threat intelligence

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.7 and the following additional guidance apply.

Guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should identify information relating to information security threats and include it in their threat intelligence process. The information or its sources can be given by the cloud service provider.	The cloud service provider should make information related to information security threats available to cloud service customers to improve overall threat intelligence processes.

5.8 Information security in project management

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.8 and the following additional guidance apply.

Guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should determine its information security requirements for the cloud service and then evaluate whether services offered by a cloud service provider can meet these requirements. For this evaluation, the cloud service customer should request	The cloud service provider should provide information to the cloud service customers about the information security capabilities used by the cloud service customer. This information should be informative without disclosing

information on the information security capabilities from the cloud service provider.	information that could be useful to someone with malicious intent.

Other information for cloud services

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

5.9 Inventory of information and other associated assets

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.9 and the following additional guidance apply.

Guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer'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.	The inventory of information and other associated assets of the cloud service provider should explicitly identify: — cloud service customer data; — cloud service derived data.

Other information for cloud services

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

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

5.10 Acceptable use of information and other associated assets

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

5.11 Return of assets

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.11 and the following additional guidance apply.

Guidance for cloud services

Cloud service customer	Cloud service provider
Before starting to use a cloud service, cloud service customer should confirm that its own assets on the cloud computing environment used for the service, especially cloud service derived data, will be returned	The cloud service provider should clearly state to the cloud service customer if the cloud service customer'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 cloud service customer. The cloud service provider should return the cloud service

or not upon the termination of use of the cloud service.	customer's assets when requested according to the agreements.

Other information for cloud services

See also 8.10 for the case which needs information deletion.

5.12 Classification of information

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

5.13 Labelling of information

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.13 and the following additional guidance apply.

Guidance for cloud services

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

5.14 Information transfer

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

5.15 Access control

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

5.16 Identity management

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.16 and the following additional guidance apply.

Guidance for cloud services

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

Other information for cloud services

The cloud service provider should support third party identity and access management technologies for its cloud services and the associated administration interfaces. These technologies can enable easier

integration and easier user identity administration between the cloud service customer's systems and the cloud service, and can ease the use of multiple cloud services, supporting such capabilities as single sign-on.

5.17 Authentication information

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.17 and the following additional guidance apply.

Guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should verify that the cloud service provider's procedure for managing authentication information, such as passwords, PIN, security token, biometrics, meets the cloud service customer's requirements.	The cloud service provider should provide information on procedures it provides for the management of the authentication information of the cloud service customer, including the procedures for allocating such information.

5.18 Access rights

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.18 and the following additional guidance apply.

Guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should verify that the cloud service access right capabilities meet the cloud service customer's requirements.	The cloud service provider should provide functions for managing the access rights of the cloud service customer's cloud service users, and specifications for the use of these functions.

5.19 Information security in supplier relationships

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

5.20 Addressing information security within supplier agreements

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.20 and the following additional guidance apply.

Guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should ensure that the service agreement includes the information security roles and responsibilities relating to the cloud. These can include the following processes: — malware protection; — backup; — cryptographic control;	The cloud service provider should specify as part of an agreement the relevant information security measures that the cloud service provider implements. The relevant information security measures that the cloud service provider will implement can vary based on the type of cloud service the cloud service customer is using.

— vulnerability management; — incident management; — technical compliance checking; — security testing; — auditing; — collection, maintenance and protection of evidence, including logs and audit trails; — protection of information upon termination of the service agreement; — authentication and access control; — identity and access management; — continuous monitoring.	The cloud service provider should describe in the service agreement the information security roles and responsibilities relating to the cloud service. These can include the following processes: — malware protection; — backup; — cryptographic control; — vulnerability management; — incident management; — technical compliance checking; — security testing; — auditing; — collection, maintenance and protection of evidence, including logs and audit trails; — protection of information upon termination of the service agreement; — authentication and access control; — identity and access management; — continuous monitoring.

5.21 Managing information security in the ICT supply chain

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.21 and the following additional guidance apply.

Guidance for cloud services

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

5.22 Monitoring, review and change management of supplier services

The 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 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 control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.24 and the following additional guidance apply.

Guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should ensure that the allocation of responsibilities the process and the procedures for information security incident management are agreed with the cloud service provider. The cloud service customer should verify the following: — the scope of information security incidents that the cloud service provider will report to the cloud service customer; — the target time period in which notifications of information security incidents will occur from the cloud service provider to the cloud service customer; — the procedure for the notification of information security incidents from the cloud service provider to the cloud service customer; — 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 cloud service provider should define the allocation of information security incident management responsibilities and procedures between the cloud service customer and the cloud service provider. The cloud service provider should provide the cloud service customer with documentation covering: — the scope of information security incidents that the cloud service provider will report to the cloud service customer; — 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 apply if certain information security incidents occur.

5.25 Assessment and decision on information security events

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

5.26 Response to information security incidents

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

5.27 Learning from information security incidents

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

5.28 Collection of evidence

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.28 and the following additional guidance apply.

Guidance for cloud services

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

5.29 Information security during disruption

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

5.30 ICT readiness for business continuity

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.30 and the following additional guidance apply.

Guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should ensure that: a) the service level regarding service interruption or disruption of the cloud service which are defined in cloud SLA or other agreements meets the RTO determined by the cloud service customer; b) the cloud service's backup functionality provided for the cloud service customer can support the RPO for data recovery required for the ICT strategy in the event of business interruption or disruption. The cloud service customer should consider redundancy, such as using other cloud services or ICT environments.	The cloud service provider should document cloud SLA or other agreement and agree with the cloud service customer. The cloud service provider should define information about the business continuity of the cloud services in advance, and provide the information to the cloud service customer.

5.31 Identification of legal, statutory, regulatory and contractual requirements

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.31 and the following additional guidance apply.

Guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should identify laws and regulations governing the cloud service provider, and evaluate if they are consistent with the obligations of the cloud service customer. The cloud service customer should request evidence of the cloud service provider's compliance with relevant regulations and standards required for the cloud service customer's business. Such evidence can be the certifications produced by third-party	The cloud service provider should inform the cloud service customer of the legal jurisdictions governing the cloud service. The cloud service provider should identify its own relevant legal requirements (e.g. regarding encryption to protect personally identifiable information (PII)). This information can be provided to the cloud service customer if appropriate. The cloud service provider should provide the

auditors. The cloud service customer should verify that the set of cryptographic controls applied by the cloud service provider comply with the agreements, legislation and regulations applicable to the cloud service customer.	cloud service customer with evidence of its current compliance with applicable legislation and contractual requirements. The cloud service provider should provide descriptions of the cryptographic controls implemented by the cloud service provider to the cloud service customer. The cloud service provider should inform the cloud service customer of the geographical locations of the cloud service provider's organization and the countries where the cloud service provider can store and process the cloud service customer data and cloud service derived data.

Other information for cloud services

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

5.32 Intellectual property rights

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.32 and the following additional guidance apply.

Guidance for cloud services

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

5.33 Protection of records

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.33 and the following additional guidance apply.

Guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should request information from the cloud service provider	The cloud service provider should provide information to the cloud service customer about

about the protection of records gathered, stored, and archived by the cloud service provider that are relevant to the use of cloud services by the cloud service customer.	the protection of records that are gathered and stored by the cloud service provider relating to the use of cloud services by the cloud service customer.

5.34 Privacy and protection of PII

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.34 apply.

Other information for cloud services

ISO/IEC 27018 offers additional information on this topic.

5.35 Independent review of information security

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.35 and the following additional guidance apply.

Guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer 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 cloud service provider. Such evidence can include certifications against relevant standards.	The cloud service provider should provide documented evidence to the cloud service customer to substantiate its claim of implementing information security controls. Where individual cloud service customer audits are impractical or can increase risks to information security, the cloud service provider should provide independent evidence that information security is implemented and operated in accordance with the cloud service provider's policies and procedures. This should be made available to prospective cloud service customers prior to entering a contract. A relevant independent audit as selected by the cloud service provider should normally be an acceptable method for fulfilling the cloud service customer's interest in reviewing the cloud service provider's operations, provided sufficient transparency is provided. When the independent audit is impractical, the cloud service provider should conduct a self-assessment, and disclose its process and results to the cloud service customer.

5.36 Compliance with policies and standards for information security

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

5.37 Documented operating procedures

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 5.37 apply.

6 Cloud service specific guidance related to people controls

6.1 Screening

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

6.2 Terms and conditions of employment

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

6.3 Information security awareness, education and training

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 6.3 and the following additional guidance apply.

Guidance for cloud services

Cloud service customer	Cloud service provider
Information security awareness, education and training programmes about cloud services should be provided to management and the supervising managers, including those of business units, cloud service administrators, cloud service integrators and cloud service users, 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, 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 cloud service provider should provide awareness, education and training for personnel, and require relevant interested parties to do the same, concerning the appropriate handling of cloud service customer data and cloud service derived data. This data can contain information confidential to a cloud service customer or be subject to specific limitations, including regulatory restrictions, on access and use by the cloud service provider.

6.4 Disciplinary process

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

6.6 Confidentiality or non-disclosure agreements

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

6.7 Remote working

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

6.8 Information security event reporting

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 6.8 and the following additional guidance apply.

Guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should request information from the cloud service provider about the mechanisms for: — the cloud service customer to report an information security event it has detected to the cloud service provider; — the cloud service provider to report an information security event it has detected to the cloud service customer; — the cloud service customer to track the status of a reported information security event.	The cloud service provider should provide mechanisms for: — the cloud service customer to report an information security event to the cloud service provider; — the cloud service provider to report an information security event to the cloud service customer; — the cloud service customer to track the status of a reported information security event.

7 Cloud service specific guidance related to physical controls

7.1 Physical security perimeter

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

7.2 Physical entry controls

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

7.3 Securing offices, rooms and facilities

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

7.4 Physical security monitoring

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

7.5 Protecting against physical and environmental threats

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

7.6 Working in secure areas

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

7.7 Clear desk and clear screen

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

7.8 Equipment siting and protection

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

7.9 Security of assets off-premises

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

7.10 Storage media

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

7.11 Supporting utilities

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

7.12 Cabling security

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

7.13 Equipment maintenance

The 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 control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 7.14 and the following additional guidance apply.

Guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should request confirmation that the cloud service provider has the policies and procedures for secure disposal or re-use of resources.	The cloud service provider should provide the cloud service customer with information about the process and methods for the secure disposal or re-use of resources (e.g. equipment, data storage, files, memory).

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

8.2 Privileged access rights

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.2 and the following additional guidance apply.

Guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should use appropriate authentication techniques for elevated privileges (e.g., multi-factor authentication) for authenticating the cloud service administrators of the cloud service customer.	The cloud service provider should provide sufficient authentication techniques for elevated privileges for authenticating the cloud service administrators of the cloud service customer to the administrative capabilities of a cloud service, according to the identified risk. For example, the

	cloud service provider can provide multi-factor authentication capabilities or enable the use of third party multi-factor authentication mechanisms.

8.3 Information access restriction

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.3 and the following additional guidance apply.

Guidance for cloud services

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

Other information for cloud services

The cloud computing environment includes additional areas that require access controls. As part of the cloud service or cloud service functions, access to functions and services, such as the hypervisor management functions and administrative consoles, should have additional access control. Both the cloud service customer and the cloud service provider may have responsibilities to these additional areas for access controls.

8.4 Access to source code

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

8.5 Secure authentication

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

8.6 Capacity management

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.6 and the following additional guidance apply.

Guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should ensure that the capacity provided by the cloud service provider meets the cloud service customer's requirements. The cloud service customer should monitor the use of cloud services, and forecast their	The cloud service provider should monitor their total resource capacity to prevent information security incidents caused by resource shortages. The cloud service provider should provide to the cloud service customer tools for monitoring the capacity. The cloud service provider should

capacity needs, to ensure performance of the cloud services over time. In order for the cloud service customer to perform capacity management for cloud services, the cloud service customer should have access to relevant statistics on resource usage, such as: — statistics for particular time periods; — maximum levels of resource usage.	provide information to the cloud service customer, in the cloud service agreement, if these tools are not available or the cloud service customer is expected to pay for these tools.

Other information for cloud services

Cloud services involve resources that are under the control of the cloud service provider and made available to the cloud service customer under the terms of the master service agreement and a related SLA. These resources include software, processing hardware, data storage, and network connectivity. Elastic, scalable and on-demand allocation of resources in a cloud service generally increases the total capacity of the service. However, the resources assigned to the cloud service customer could have capacity constraints. Examples of capacity constraints include the number of processor cores for an application, the amount of storage available, or the network bandwidth available. The constraints can vary depending on the particular cloud service or the particular subscription that the cloud service customer purchases. If the cloud service customer has requirements that exceed the constraints, the cloud service customer might need to change the cloud service or change the subscription.

8.7 Protection against malware

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

8.8 Management of technical vulnerabilities

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.8 and the following additional guidance apply.

Guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should request information from the cloud service provider about the management of technical vulnerabilities that can affect the cloud services provided. The cloud service customer should identify which technical vulnerabilities they are responsible for, and clearly define their processes for managing them.	The cloud service provider should make available to the cloud service customer information about the management of technical vulnerabilities that can affect the cloud services provided.

8.9 Configuration management

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.9 and the following additional guidance apply.

Guidance for cloud services

Cloud service customer	Cloud service provider

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

Other information for cloud services

When configuring virtual environments, cloud service customers and cloud service providers should ensure that appropriate aspects are hardened (e.g., only those ports, protocols and services that are needed), and that the appropriate technical measures are in place (e.g., anti-malware, logging) for each virtual machine used.

For more information on the monitoring of cloud services for the purpose of configuration management, see Annex C.

8.10 Information deletion

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.10 and the following additional guidance apply.

Guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should request a documented description of the termination of service process that covers removal of cloud service customer's assets followed by the deletion of all copies of those assets from the cloud service provider's systems. The description should list all the assets	The cloud service provider should provide information about the arrangements for the removal of any cloud service customer's assets upon termination of the agreement for the use of a cloud service. The asset removal arrangements should be documented in the agreement and should be performed in a timely manner. The

including cloud service customer data and cloud service derived data and document the schedule for the termination of service, which should occur in a timely manner.	arrangements should specify the assets to be removed, including cloud service customer data and cloud service derived data..

Other information for cloud services

See also 5.11 for the case which needs return of assets of the cloud service customer.

8.11 Data masking

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.11 and the following additional guidance apply.

Guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should confirm that if data masking is required, it can be performed by the cloud service. When using the data masking functionality provided by the cloud service, the cloud service customer should verify that the functionality is in compliance with the cloud service customer's topic-specific policies on data masking. If the data masking provided by the cloud service does not comply with the topic-specific policy on data masking, the cloud service customer should either stop using the cloud service or upload its own masked data to the cloud service.	When the cloud service provider provides data masking capability of the cloud service for the cloud service customer, the cloud service provider should provide information about such capabilities.

8.12 Data leakage prevention

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

8.13 Information backup

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.13 and the following additional guidance apply.

Guidance for cloud services

Cloud service customer	Cloud service provider
Where the cloud service provider provides backup capability as part of the cloud service, the cloud service customer should request the specifications of the backup capability from the cloud service provider. The cloud service customer should verify	The cloud service provider should provide the specifications of its backup capabilities to the cloud service customer. The specifications should include the following information, as appropriate: — scope and schedule of backups;

that the backup capability meets the cloud service customer's backup requirements. The cloud service customer is responsible for implementing backup capabilities, when the backup capabilities provided by the cloud service provider do not meet the cloud service customer's requirements.	— 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 service is offered to the cloud service customer, the cloud service provider should provide secure and segregated access to backups, such as virtual snapshots.

Other information for cloud services

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

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

8.14 Redundancy of information processing facilities

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

8.15 Logging

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.15 and the following additional guidance apply.

Guidance for cloud services

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

Other information for cloud services

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

8.16 Monitoring activities

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.16 and the following additional guidance apply.

Guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should request information from the cloud service provider of the service monitoring capabilities available for each cloud service.	The cloud service provider should provide capabilities that enable the cloud service customer to monitor specified aspects, relevant to the cloud service customer, of the operation of the cloud services. For example, to monitor and detect if the cloud service is being used as a platform to attack others, or if traffic data shows abnormal behaviour. Appropriate access controls should secure the use of the monitoring capabilities. The capabilities should provide access only to information about the cloud service customer's own cloud service instances. The cloud service provider should provide description of the service monitoring capabilities to the cloud service customer. Monitoring should provide data consistent with the logs described in clause 8.15 and assist with cloud SLA terms.

Other information for cloud services

For more information on the monitoring of cloud services, see Annex C.

8.17 Clock synchronization

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.17 and the following additional guidance apply.

Guidance for cloud services

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

Other information for cloud services

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

8.18 Use of privileged utility programs

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.18 and the following additional guidance apply.

Guidance for cloud services

Cloud service customer	Cloud service provider
Where the use of utility programs is permitted, the cloud service customer should identify the utility programs to be used in its cloud computing environment and ensure that they do not interfere with the controls of the cloud service.	The cloud service provider should identify the requirements for any utility programs which the cloud service customer is authorized to operate in the cloud service customer's environment.

8.19 Installation of software on operational systems

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

8.20 Network controls

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.20 and the following additional guidance apply.

Guidance for cloud services

Cloud service customer	Cloud service provider
(no additional guidance)	The cloud service provider 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 cloud service provider 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.

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 network can cause system outages or defective access control.

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

8.21 Security of network services

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

8.22 Segregation in networks

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

8.23 Web filtering

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

8.24 Use of cryptography

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.24 and the following additional guidance apply.

Guidance for cloud services

Cloud service customer	Cloud service provider
When the cloud service provider offers cryptography, the cloud service customer should review any information supplied by the cloud service provider to confirm whether the cryptographic capabilities: — meet the cloud service customer's information security requirements of cryptography; — are compatible with any other cryptographic protection used by the cloud service customer; — apply to data at rest and in transit to, from and within the cloud service. Where the cloud service provider provides key management functionality for use by the cloud service customer, the cloud service customer should request the following information on the procedures used to manage keys related to the cloud service: — type of keys; — specifications of the key management system, including procedures for each stage of the key life-cycle, i.e., generating, changing or updating, storing, retiring, retrieving, retaining and destroying; — recommended key management procedures for use by the cloud service customer. The cloud service customer should not permit the cloud service provider to store and manage the encryption keys for cryptographic operations when the cloud service customer employs its own key management or a separate and distinct key management service.	The cloud service provider should provide information to the cloud service customer regarding the circumstances in which it uses cryptography to protect the information it processes. The cloud service provider should also provide information to the cloud service customer about any capabilities it provides that can assist the cloud service customer in applying its own cryptographic protection.

8.25 Secure development lifecycle

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.25 and the following additional guidance apply.

Guidance for cloud services

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

Other information for cloud services

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

8.26 Application security requirements

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

8.27 Secure system architecture and engineering principles

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

8.28 Secure coding

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

8.29 Security testing in development and acceptance

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

Other information for cloud services

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

8.30 Outsourced development

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

8.32 Change management

The control, purpose, guidance and other information stated in ISO/IEC 27002:2022, 8.32 and the following additional guidance apply.

Guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer's change management process should take into account the impact of any changes made by the cloud service provider in correction with	The cloud service provider should provide the cloud service customer with information regarding changes to the cloud service that could adversely affect the cloud service. The following

changes made by the cloud service customer.	will help the cloud service customer determine the effect the changes can have 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 a cloud service provider offers a cloud service that depends on a peer cloud service provider, then the cloud service provider might need to inform the cloud service customer of changes caused by the peer cloud service provider.

Other information for cloud services

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

8.33 Test information

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

Annex A
(normative)

Cloud service extended control set

This annex provides additional controls, purposes, guidance and other information as an extended control set for cloud services. An organization intending to implement these controls in an information security management system (ISMS) that is to be conformant to ISO/IEC 27001, should extend its statement of applicability (SOA) by including the controls stated in this annex.

NOTE Each control in ISO/IEC 27002:2022 and this document is associated with five attributes, i.e. Control types, Information security properties, Cybersecurity concepts, Operational capabilities, and Security domains, with corresponding attribute values. An organization can define attributes and attribute values to create its own views of controls.

CLD.5.38 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

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 cloud service customer and the cloud service provider.

Purpose

To clarify the relationship regarding shared roles and responsibilities between the cloud service customer and the cloud service provider for information security management.

Guidance for cloud services

Cloud service customer	Cloud service provider
<u>Agreement</u> The cloud service customer should accept the information security roles and responsibilities as defined by the cloud service provider, 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. <u>Management of relationship with the cloud service provider</u> The cloud service customer should identify and manage its relationship with the	<u>Agreement</u> The cloud service provider should define and document the allocation of information security roles and responsibilities, and agree with its cloud service customers, its cloud service providers, and its suppliers. <u>Information provision</u> The cloud service provider should provide information to the cloud service customer regarding its information security capabilities of the cloud service and information security measures taken by the cloud service provider to assist the cloud service customer to understand

customer support function of the cloud service provider. Information request The cloud service customer should request information from the cloud service provider regarding the information security capabilities of the cloud service provider such as authentication, cryptography, backup and logging. The cloud service customer can use frameworks established by third parties or independent bodies to complement the cloud service provider information on available security capabilities.	them clearly and adequately. In order to fulfil this purpose, the cloud service provider can provide the information in accordance with frameworks established by third parties or independent bodies.

Other information for cloud services

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

CLD.5.39 Administrator's operational security

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management, #Information_protection, #System_and_network_security, #Application_security, #Secure_configuration, #Identity_and_access_management, #Threat_and_vulnerability_management, #Continuity, #Supplier_relationships_security, #Information_security_event_management	#Protection

Control

Procedures for administrative operations of a cloud computing environment should be defined, documented, and monitored.

Purpose

To avoid administrative error for critical operations in the use of a cloud service.

Guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer 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 devices such as servers, networks and storage; — termination procedures for cloud service usage; — backup and restoration. The document should specify that a supervisor should monitor these operations.	The cloud service provider should provide documentation about the critical operations and procedures to cloud service customers who require it.

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 cloud service customer and the cloud service provider. Because 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.

Examples of the critical operations are:

— installation, changes, and deletion of virtualized;

— devices such as servers, networks and storage;

— termination procedures for cloud service usage;

— backup and restoration.

CLD.5.40 Agreement of roles and responsibilities of the cloud service partner

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

Control

Roles and responsibilities for information security of the cloud service partner should be clarified and agreed upon with the users of the cloud service partner's service.

Purpose

To delineate the roles and responsibilities of the cloud service provider and the cloud service customer when using a cloud service partner.

01 **Guidance for cloud services**

Cloud service customer	Cloud service provider
The cloud service customer and/or cloud service provider using the cloud service partner should clearly define and agree with the cloud service partner on the roles and responsibilities to be assumed by the cloud service partner. When signing an agreement, it should be ensured that the roles and responsibilities of each organization are precisely defined between the cloud service partner and the cloud service customer, or between the cloud service partner and the cloud service provider.	

02 ## CLD.8.35 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	#Governance_and_Ecosystem #Protection

03 **Control**

04 A cloud service customer's virtual environment running on a cloud service should be protected from
05 other cloud service customers and unauthorized persons.

06 **Purpose**

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

08 **Guidance for cloud services**

Cloud service customer	Cloud service provider
The cloud service customer should define its requirements for segregating the cloud service customers' environments to achieve tenant isolation in the shared virtual environment of the cloud service and verify that the cloud service provider meets those requirements.	The cloud service provider should enforce appropriate logical segregation of cloud service customer data, virtualized applications, operating systems, storage, and network for the separation of resources used by cloud service customers in multi-tenant environments to ensure appropriate isolation of resources used by different tenants. Where the cloud service involves multi-tenancy, the cloud service provider should implement information security controls to ensure appropriate isolation of resources used by different tenants. The cloud service provider should consider the risks associated with running cloud service customer-supplied software within the cloud services offered by the cloud service provider.

09 **Other information for cloud services**

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

Implementation of the 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 cloud service customers 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.

CLD.8.36 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	#Information_security_event_management	#Protection #Defence

Control

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

Purpose

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

Guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should consider implementing: a) monitoring and logging cloud service users' access and activities of the cloud service customers to cloud services; b) periodic compliance checking with the information security policy, topic-specific policy on the use of cloud services and relevant rules and standards; c) monitoring and prevention of unintended or unauthorised information transfer to and from the cloud service environment managed by the cloud service customer; d) detection of anomalies, such as increasing resource utilization and unknown service usages by detecting deviations from normal conditions. In addition to monitoring the use of individual cloud services of specific tenant or region, a control should be implemented for any tenants and regions where the cloud service customer activated to use to detect anomaly, such as increasing resource utilization and unknown service usages by detecting deviations from	The cloud service provider should provide the cloud service customer with guidance and functions to monitor and control cloud service users' use of the cloud service.

normal conditions using machine learning or AI technologies.	

26

Annex B
(informative)

Correspondence with ISO/IEC 27017:2015

The purpose of this annex is to provide backwards compatibility with ISO/IEC 27017:2015 for organizations that are currently using that standard and now wish to transition to this edition.

Table B.1 provides the correspondence of the controls specified in Clauses 5 to 8 with those in ISO/IEC 27017:2015. The listed controls are those which have guidance and other information for cloud services only. The note "New" in Table B.1 means that the control is added in ISO/IEC 27002:2022 or the cloud service specific control with "CLD" is added in this edition of ISO/IEC 27017.

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

ISO/IEC 27017:202X control identifier	ISO/IEC 27017:2015 control identifier	Control name
5.1	5.1.1	Policies for information security
5.2	6.1.1	Information security roles and responsibilities
5.5	6.1.3	Contact with authorities
5.7	New	Threat intelligence
5.8	14.1.1	Information security in project management
5.9	8.1.1, 8.1.2	Inventory of information and other associated assets
5.11	New	Return of assets
5.13	8.2.2	Labelling of information
5.16	9.2.1	Identity management
5.17	9.2.4	Authentication information
5.18	9.2.2	Access rights
5.20	15.1.2	Addressing information security within supplier agreements
5.21	15.1.3	Managing information security in the ICT supply chain
5.24	16.1.1	Information security incident management planning and preparation
5.28	16.1.7	Collection of evidence
5.30	New	ICT readiness for business continuity
5.31	18.1.5	Legal, statutory, regulatory and contractual requirements
5.33	18.1.3	Protection of records
5.35	18.2.1	Independent review of information security
6.3	7.2.2	Information security awareness, education and training
6.8	16.1.2	Information security event reporting

Table B.1 (*continued*)

ISO/IEC 27017:202X control identifier	ISO/IEC 27017:2015 control identifier	Control name
7.14	11.2.7	Secure disposal or re-use of equipment
8.2	9.2.3	Privileged access rights
8.3	9.4.1	Information access restriction
8.6	12.1.3	Capacity management
8.8	12.6.1	Management of technical vulnerabilities
8.9	New	Configuration management
8.10	New	Information deletion
8.11	New	Data masking
8.13	12.3.1	Information backup
8.15	12.4.1, 12.4.3	Logging
8.16	New	Monitoring activities
8.17	12.4.4	Clock synchronization
8.18	9.4.4	Use of privileged utility programs
8.20	13.1.1	Networks security
8.24	10.1.1, 10.1.2	Use of cryptography
8.25	14.2.1	Secure development life cycle
8.32	12.1.2	Change management
CLD.5.38	CLD.6.3.1	Shared roles and responsibilities within a cloud computing environment
CLD.5.39	CLD.12.1.5	Administrator's operational security
CLD.5.40	New	Agreement of roles and responsibilities of the cloud service partner
CLD.8.35	CLD.9.5.1	Segregation in virtual computing environments
CLD.8.36	New	Detect and prevent unauthorized use of cloud services

Table B.2 provides the correspondence of controls specified in ISO/IEC 27017:2015 with those in this document. The listed controls are those which have guidance and other information for cloud services only. The control marked with “Removed” are either:

- a control of ISO/IEC 27002:2013 which has implementation guidance or other information for cloud services, but corresponding control of ISO/IEC 27002:2022 does not;
- a cloud service specific control (“CLD”) of ISO/IEC 27017:2015 which has not corresponding control in this edition of ISO/IEC 27017.

850 **Table B.2 – Correspondence between controls in ISO/IEC 27002:2013 and controls**
851 **in this document**

ISO/IEC 27017:2015 control identifier	ISO/IEC 27017:202X control identifier	Control name
5		Information security policies
5.1		Management direction for information security
5.1.1	5.1	Policies for information security
6		Organization of information security
6.1		Internal organization
6.1.1	5.2	Information security roles and responsibilities
6.1.3	5.5	Contact with authorities
7		Human resource security
7.2		During employment
7.2.2	6.3	Information security awareness, education and training
8		Asset management
8.1		Responsibility for assets
8.1.1	5.9	Inventory of assets
8.1.2	5.9	Ownership of assets
8.2		Information classification
8.2.2	5.13	Labelling of information
9		Access control
9.1		Business requirements of access control
9.1.2	Removed	Access to networks and network services
9.2		User access management
9.2.1	5.16	User registration and deregistration
9.2.2	5.18	User access provisioning
9.2.3	8.2	Management of privileged access rights
9.2.4	5.17	Management of secret authentication information of users
9.4		System and application access control
9.4.1	8.3	Information access restriction
9.4.4	8.18	Use of privileged utility programs
10		Cryptography
10.1		Cryptographic controls
10.1.1	8.24	Policy on the use of cryptographic controls

52 **Table B.2 (*continued*)**

ISO/IEC 27017:2015 control identifier	ISO/IEC 27017:202X control identifier	Control name
10.1.2	8.24	Key management
11		Physical and environmental security
11.2		Equipment
11.2.7	7.14	Secure disposal or reuse of equipment
12		Operations security
12.1		Operational procedures and responsibilities
12.1.2	8.32	Change management
12.1.3	8.6	Capacity management
12.3		Backup
12.3.1	8.13	Information backup
12.4		Logging and monitoring
12.4.1	8.15	Event logging
12.4.3	8.15	Administrator and operator logs
12.4.4	8.17	Clock synchronization
12.6		Technical vulnerability management
12.6.1	8.8	Management of technical vulnerabilities
13		Communications security
13.1		Network security management
13.1.3	Removed	Segregation in networks
14		System acquisition, development and maintenance
14.1		Security requirements of information systems
14.1.1	5.8	Information security requirements analysis and specification
14.2		Security in development and support processes
14.2.1	8.25	Secure development policy
14.2.9	8.29	System acceptance testing
15		Supplier relationships
15.1		Information security in supplier relationships
15.1.1	5.19	Information security policy for supplier relationships
15.1.2	5.20	Addressing security within supplier agreements
15.1.3	5.21	Information and communication technology supply chain
16		Information security incident management

853 **Table B.2 (*continued*)**

ISO/IEC 27017:2015 control identifier	ISO/IEC 27017:202X control identifier	Control name
16.1		Management of information security incidents and improvements
16.1.1	5.24	Responsibilities and procedures
16.1.2	6.8	Reporting information security events
16.1.7	5.28	Collection of evidence
17		Information security aspects of business continuity management
18		Compliance
18.1		Compliance with legal and contractual requirements
18.1.1	5.31	Identification of applicable legislation and contractual requirements
18.1.2	5.32	Intellectual property rights
18.1.3	5.33	Protection of records
18.1.4	5.34	Privacy and protection of personally identifiable information
18.1.5	5.31	Regulation of cryptographic controls
18.2		Information security reviews
18.2.1	5.35	Independent review of information security
CLD.6.3		Relationship between cloud service customer and cloud service provider
CLD.6.3.1	CLD.5.38	Shared roles and responsibilities within a cloud computing environment
CLD8.1.5	Removed	Removal of cloud service customer assets
CLD9.5		Access control of cloud service customer data in shared virtual environment
CLD.9.5.1	CLD.8.35	Segregation in virtual computing environments
CLD.9.5.2	Removed	Virtual machine hardening
CLD.12.1.5	CLD.5.39	Administrator's operational security
CLD.12.4.5	Removed	Monitoring of Cloud Services
CLD.13.1.4	Removed	Alignment of security management for virtual and physical networks

854

Annex C
(informative)

Monitoring of cloud services

C.1 Monitoring of cloud services

Cloud computing, amongst others, 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, collecting, reviewing, and evaluating logs for sources of potential issues. These tasks could be performed manually or automatically through software tools. Although these tasks could be performed through a third party (e.g. IT Services supplier), the same process was 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 cloud service customer (depending on the service model, this could range from insubstantial – SaaS – to increased – IaaS). The cloud service customer and the cloud service provider have specific roles and responsibilities regarding monitoring, either for the detection of security-relevant events or for configuration management purposes. For example, when a cloud service customer uses SaaS, they have a limited number of security monitoring functions that can be implemented, and they are only related to the internal functions of the software (e.g. in a CRM application they may see business related information submitted by the personnel of the organization). In contrast, consider the example of an IaaS cloud service customer who leverages specific tools (where a broader number of functions are implemented) to continuously monitor if the standard configuration templates offered by the cloud service provider satisfy a security policy. In both examples, the cloud service customer has no monitoring capabilities on the infrastructure (logical or hardware) that supports the provision of the cloud service. In these cases, the cloud service customer (depending also on the agreed upon terms of service) will have to content with the information shared by the cloud service provider (see CLD.5.38).

Monitoring of the cloud service for configuration management purposes is expected to rely on "automated monitoring" or "monitoring with automation" i.e., gathering and pre-processing data by non-human means. Automated monitoring should be distinguished from continuous monitoring. The latter refers to monitoring for an enduring period of time that can be applied both with or without automation. The introduction of automated monitoring for configuration management activities can leverage available technology (e.g., Cloud Security Posture Management) and machine-readable languages (e.g, Open Security Controls Assessment Language (OSCAL)) able to manage the complexity and scale of cloud services.

In the mid-term, "automated monitoring" might facilitate processes and practices of auditing cloud services. Since audit 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 limitation of available information, mandates that the audit plans and relevant risk treatment options are adapted and supported with available tools (e.g. for the above mentioned SaaS example and for the criterion related to access control, an auditor would need to collect and evaluate evidence for the access control within the SaaS application and for the rest the collected evidence could be just the relevant agreements of the cloud service).

As different service models introduce differences in the responsibilities and abilities for monitoring and auditing between the cloud service customer and the cloud service provider, SaaS often offers the most limited auditing and monitoring capabilities for the cloud service customer while proving the most extensive capabilities for the cloud service provider.

In conclusion, for the cloud service customer, within the project of cloud computing transition, the monitoring and configuration management should be implemented and supported by automated

903 monitoring. For the cloud service provider, on the other hand, monitoring and configuration management
904 should cover their own needs for the effective and efficient operation of the relevant services as well as
905 make provisions for the needs for information of the cloud service customer.

Bibliography

[1] ISO/IEC 5140 *Information technology — Cloud computing — Concepts for multi-cloud and multiple cloud services*

[2] ISO/IEC 19440:2020, *Enterprise modelling and architecture — Constructs for enterprise modelling*

[3] ISO/IEC 22123-1:2023, *Information technology — Cloud computing — Part 1: Vocabulary*

[4] ISO/IEC 22123-3:2023, *Information technology — Cloud computing — Part 3: Reference architecture*

[5] ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

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

[7] ISO/IEC 27005, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*

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

[9] ISO/IEC 27036-4, *Information technology — Security techniques — Information security for supplier relationships — Part 4: Guidelines for security of cloud services*

[10] ISO/IEC 27040, *Information technology — Security techniques — Storage security*

[11] ISO 31000, *Risk management — Guidelines*