International Standard

ISO/IEC 27018

Third edition
2025-08

Information security, cybersecurity and privacy protection — Guidelines for protection of personally identifiable information (PII) in public clouds acting as PII processors

Sécurité de l'information, cybersécurité et protection de la vie privée — Lignes directrices en matière de protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII

Reference number
ISO/IEC 27018:2025(en)

COPYRIGHT PROTECTED DOCUMENT

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

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

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

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

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

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This third edition cancels and replaces the second edition (ISO/IEC 27018:2019), which has been technically revised.

The main changes are as follows:

— the text has been aligned with ISO/IEC 27002:2022;

— Annex B has been added.

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

Introduction

0.1 Background and context

Cloud service providers who process personally identifiable information (PII) under contract to their customers are expected to operate their services in ways that allow both parties to meet the requirements of applicable legislation and regulations covering the protection of PII. The requirements and the way in which the requirements are divided between the cloud service provider and its customers vary according to legal jurisdiction, and according to the terms of the contract between the cloud service provider and the customer. Legislation which governs how PII is allowed to be processed (i.e. collected, used, transferred and disposed of) is sometimes referred to as data protection legislation; PII is sometimes referred to as personal data or personal information. The obligations falling on a PII processor vary from jurisdiction to jurisdiction, which makes it challenging for businesses providing cloud computing services to operate in a multinational environment.

A public cloud service provider is a "PII processor" when it processes PII for and according to the instructions of a cloud service customer. The cloud service customer, who has the contractual relationship with the public cloud PII processor, can range from a natural person (i.e. a "PII principal", processing his or her own PII in the cloud) to an organization (i.e. a "PII controller", processing PII relating to many PII principals). The cloud service customer can authorize one or more cloud service users associated with it to use the services made available to the customer under its contract with the public cloud PII processor. The cloud service customer has authority over the processing and use of the data. A cloud service customer who is also a PII controller can be subject to a wider set of obligations governing the protection of PII than the public cloud PII processor. Maintaining the distinction between PII controller and PII processor relies on the public cloud PII processor having no data processing objectives other than those set by the cloud service customer with respect to the PII it processes and the operations necessary to achieve the cloud service customer's objectives.

NOTE 1 Where the public cloud PII processor is processing cloud service customer account data, it can be acting as a PII controller for this purpose. This document does not cover such activity.

The intention of this document, when used in conjunction with the information security objectives and controls in ISO/IEC 27002, is to create a common set of security categories and controls that can be implemented by a public cloud computing service provider acting as a PII processor. This document has the following objectives:

— to enable the public cloud PII processor to be transparent in relevant matters so that cloud service customers can select well-governed cloud-based PII processing services;

— to assist the cloud service customer and the public cloud PII processor in entering into a contractual agreement;

— to provide cloud service customers with a mechanism for exercising audit and compliance rights and responsibilities in cases where the individual cloud service customer data, which are hosted in a multi-party, virtualized server (cloud) environment, can be technically impractical to audit and can potentially increase risks to those physical and logical network security controls in place.

NOTE 2 It is expected that public cloud service providers comply with applicable obligations when acting as a PII processor.

This document can assist by providing a common compliance framework for public cloud service providers, in particular those that operate in a multinational market.

0.2 PII protection controls for public cloud computing services

This document is designed for organizations to use as a reference for selecting PII protection controls within the process of implementing a cloud computing information security management system based on ISO/IEC 27001, or as a guidance document for implementing commonly accepted PII protection controls for organizations acting as public cloud PII processors. In particular, this document has been based on ISO/IEC 27002, taking into consideration the specific risk environment(s) arising from those PII protection requirements which can apply to public cloud computing service providers acting as PII processors.

In the context of PII protection requirements for a public cloud service provider acting as a PII processor, the organization is protecting the information assets entrusted to it by its customers. Implementation of the controls of ISO/IEC 27002 by the public cloud PII processor is both suitable for this purpose and necessary. This document extends the ISO/IEC 27002 controls to accommodate the distributed nature of the risk and the existence of a contractual relationship between the cloud service customer and the public cloud PII processor. This document extends ISO/IEC 27002 in two ways, by providing:

— implementation guidance applicable to public cloud PII protection for some of the existing ISO/IEC 27002 controls, and

— a set of additional controls and associated guidance in Annex A intended to address public cloud PII protection requirements not addressed by the existing ISO/IEC 27002 control set, organized in line with the privacy principles of ISO/IEC 29100.

Most of the controls and guidelines in this document also apply to a PII controller. However, the PII controller is, in most cases, subject to additional obligations not specified here.

0.3 PII protection requirements

It is essential that an organization identifies its requirements for the protection of PII. There are three main sources of requirement, as given below.

a) Legal and contractual requirements: One source is the legal and contractual requirements to which an organization, its trading partners, contractors and service providers are bound, as well as responsibilities concerning their socio-cultural and operating environment. It should be noted that legislation, regulations and contractual commitments made by the PII processor can mandate the selection of particular controls and can also necessitate specific criteria for implementing those controls. These requirements can vary from one jurisdiction to another.

b) Risks: Another source is derived from assessing risks to the organization associated with PII, taking into account the organization's overall business strategy and objectives. Through a risk assessment, risks are identified, their consequence and likelihood are assessed and risks are evaluated. ISO/IEC 27005 provides information security risk management guidance, including advice on risk assessment, risk acceptance, risk communication, risk monitoring and risk review. ISO/IEC 29134 provides guidelines on privacy impact assessment.

c) Corporate policies: While many aspects covered by a corporate policy are derived from legal and socio-cultural requirements, an organization can also choose voluntarily to go beyond the criteria that are derived from the requirements of a).

0.4 Selecting and implementing controls in a cloud computing environment

Controls can be selected from this document (which includes by reference the controls from ISO/IEC 27002, creating a combined reference control set for the sector or application defined by the relevant sector). If required, controls can also be selected from other control sets, or new controls can be designed to meet specific needs as appropriate.

NOTE A PII processing service provided by a public cloud PII processor can be considered as an application of cloud computing rather than as a sector in itself. Nevertheless, the term "public cloud service provider-specific" is used in this document, as this is the conventional term used within other Information Security Management systems standards developed by ISO/IEC JTC 1/SC 27.

The selection of controls is dependent on organizational decisions based on the criteria for risk acceptance, risk treatment options, and the general risk management approach applied to the organization and, through contractual agreements, its customers and suppliers. It is also subject to relevant national and international legislation. Where organizations/public cloud providers do not select the controls specified in this document, a justification should be provided.

Further, the selection and implementation of controls is dependent on the public cloud provider's actual role in the context of the whole cloud computing reference architecture (see ISO/IEC 22123-3). Many different organizations can be involved in providing infrastructure and application services in a cloud computing environment. In some circumstances, selected controls can be unique to a particular service category of

the cloud computing reference architecture. In other instances, there can be shared roles in implementing security controls. Contractual agreements are expected to specify the PII protection responsibilities of all organizations involved in providing or using the cloud services, including the public cloud PII processor, its sub-contractors and the cloud service customer.

The controls in this document can be considered as guiding principles and applicable for most organizations. They are explained in more detail in this document along with implementation guidance. Implementation can be made simpler if requirements for the protection of PII have been considered in the design of the public cloud PII processor's information system, services and operations. Such consideration is an element of the concept that is often called "privacy by design" (see References [64] and [65]).

0.5 Developing additional guidelines

This document can be regarded as a starting point for developing PII protection guidelines. It is possible that not all of the controls and guidance in this code of practice are applicable. Furthermore, additional controls and guidelines not included in this document can be required. When documents are developed containing additional guidelines or controls, it can be useful to include cross-references to clauses in this document where applicable to facilitate compliance checking by auditors and business partners.

0.6 Lifecycle considerations

PII has a natural lifecycle, from creation and origination, through to storage, processing, use and transmission, to its eventual destruction or disuse. The risks to PII can vary during its lifetime but protection of PII remains important at all stages.

PII protection requirements are expected to be taken into account as existing and new information systems are managed through their lifecycle.

Information security, cybersecurity and privacy protection — Guidelines for protection of personally identifiable information (PII) in public clouds acting as PII processors

1 Scope

This document establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect personally identifiable information (PII) in line with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.

In particular, this document specifies guidelines based on ISO/IEC 27002:2022, taking into consideration the regulatory requirements for the protection of PII which can be applicable within the context of the information security risk environment(s) of a provider of public cloud services.

This document is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which provide information processing services as PII processors via cloud computing under contract to other organizations.

The guidelines in this document can also be relevant to organizations acting as PII controllers.

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 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*

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 22123-1, ISO/IEC 27000, ISO/IEC 27002 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
data breach
compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, protected data transmitted, stored or otherwise processed

[SOURCE: ISO/IEC 27040:2024, 3.5.2]

3.2
personally identifiable information
PII
information that a) can be used to establish a link between the information and the natural person to whom such information relates, or b) is or can be directly or indirectly linked to a natural person

Note 1 to entry: The "natural person" in the definition is the *PII principal* (3.4). To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to establish the link between the set of PII and the natural person.

Note 2 to entry: This definition is included to define the term PII as used in this document. A public cloud *PII processor* (3.5) is typically not in a position to know explicitly whether information it processes falls into any specified category unless this is made transparent by the cloud service customer.

[SOURCE: ISO/IEC 29100:2024, 3.7, modified — Note 2 to entry has been added.]

3.3
PII controller
privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing *personally identifiable information (PII)* (3.2) other than natural persons who use data for personal purposes

Note 1 to entry: A PII controller sometimes instructs others [e.g. *PII processors* (3.5)] to process PII on its behalf while the responsibility for the processing remains with the PII controller.

[SOURCE: ISO/IEC 29100:2024, 3.8]

3.4
PII principal
natural person to whom the *personally identifiable information (PII)* (3.2) relates

Note 1 to entry: Depending on the jurisdiction and the particular PII protection and privacy legislation, the synonym "data subject" can also be used instead of the term "PII principal".

[SOURCE: ISO/IEC 29100:2024, 3.9, modified — Note 1 to entry has been added.]

3.5
PII processor
privacy stakeholder that processes *personally identifiable information (PII)* (3.2) on behalf of and in accordance with the instructions of a *PII controller* (3.3)

[SOURCE: ISO/IEC 29100:2024, 3.10]

3.6
PII processing
processing of PII
operation or set of operations performed on *personally identifiable information (PII)* (3.2)

Note 1 to entry: Examples of processing operations of PII include, but are not limited to, the collection, storage, alteration, retrieval, consultation, disclosure, anonymization, pseudonymization, dissemination or otherwise making available, deletion or destruction of PII.

[SOURCE: ISO/IEC 29100:2024, 3.21, modified — "PII processing" has been added as the preferred term.]

3.7
public cloud service provider
party which makes cloud services available according to the public cloud model

4 Overview

4.1 Structure of this document

This document follows the structure used in ISO/IEC 27002:2022 for the description of controls. In this aspect, the same strategy that was adopted in the earlier version of this document (ISO/IEC 27018:2019), in mirroring the controls in ISO/IEC 27002:2013,[1] has been repeated here.

Annex B provides a comparison of the two control layouts in this document and the previous edition (ISO/IEC 27018:2019).

Specifically, the following rules have been used in mirroring the controls in ISO/IEC 27002:2022 in this document. In cases where the various elements of the control layout (described in 4.2) for a control are identical, only a reference is provided to the corresponding control in ISO/IEC 27002:2022. For those controls that require additional guidance and related information in the context of public cloud PII protection, additional guidance is provided under the headings “Public cloud PII protection implementation guidance” and “Other information for public cloud PII protection” respectively. This type of guidance is also referred to using the term “Public cloud service provider-specific implementation guidance”. Besides these, additional controls and associated implementation guidance applicable to PII protection for cloud computing service providers are described in Annex A. Finally, the clause numbers in this document are aligned with the corresponding clause numbers in ISO/IEC 27002:2022.

The controls in Table 1 are organized into four themes, which correspond to the controls listed in Clauses 5 to 8 as follows:

— the theme "Public cloud service provider-specific implementation guidance is provided" corresponds to the control "Public cloud PII protection implementation guidance";

— the theme "Public cloud service provider-specific implementation guidance and other information is provided" corresponds to the control "Public cloud PII protection implementation guidance and other information for Public cloud PII protection";

— the theme "No additional public cloud service provider-specific implementation guidance or other information is provided" corresponds to the control "no specific Guidance or other information for Public cloud PII protection";

— the theme "Public cloud service provider-specific implementation guidance is provided, together with a cross-reference to control(s) in Annex A" corresponds to the control "Public cloud PII protection implementation guidance and cross-reference to control(s) in Annex A".

Table 1 — Location of public cloud service provider-specific guidance and other information for implementing controls in ISO/IEC 27002:2022

ISO/IEC 27002:2022 Control identifier	ISO/IEC 27002:2022 Control name	Theme
Clause 5 – Organizational controls		
5.1	Policies for information security	Public cloud service provider-specific implementation guidance and other information is provided.[c]
5.2	Information security roles and responsibilities	Public cloud service provider-specific implementation guidance is provided.[b]
5.3	Segregation of duties	No additional public cloud service provider-specific implementation guidance or other information is provided.[d]
5.4	Management responsibilities	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.5	Contact with authorities	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.6	Contact with special interest groups	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.7 [a]	Threat intelligence	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.8	Information security in project management	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.9	Inventory of information and other associated assets	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.10	Acceptable use of information and other associated assets	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.11	Return of assets	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.12	Classification of information	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.13	Labelling of information	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]

[a] New control introduced in ISO/IEC 27002:2022.

[b] This control is applicable as "Public cloud PII protection implementation guidance".

[c] This control is applicable as "Public cloud PII protection implementation guidance and other information for public cloud PII protection".

[d] This control is applicable as "no specific Guidance or other information for Public cloud PII protection".

[e] This control is applicable as "Public cloud PII protection implementation guidance and cross-reference to control(s) in Annex A".

Table 1 *(continued)*

ISO/IEC 27002:2022 Control identifier	ISO/IEC 27002:2022 Control name	Theme
5.14	Information transfer	Public cloud service provider-specific implementation guidance is provided. [b]
5.15	Access control	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.16	Identity management	Public cloud service provider-specific implementation guidance is provided. [b]
5.17	Authentication information	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.18	Access rights	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.19	Information security in supplier relationships	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.20	Addressing information security within supplier agreements	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.21	Managing information security in the ICT supply chain	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.22	Monitoring, review and change management of supplier services	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.23 [a]	Information security for use of cloud services	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.24	Information security incident management planning and preparation	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.25	Assessment and decision on information security events	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.26	Response to information security incidents	Public cloud service provider-specific implementation guidance is provided, together with a cross-reference to control(s) in Annex A. [e]
5.27	Learning from information security incidents	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.28	Collection of evidence	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]

[a] New control introduced in ISO/IEC 27002:2022.

[b] This control is applicable as “Public cloud PII protection implementation guidance”.

[c] This control is applicable as “Public cloud PII protection implementation guidance and other information for public cloud PII protection”.

[d] This control is applicable as “no specific Guidance or other information for Public cloud PII protection”.

[e] This control is applicable as “Public cloud PII protection implementation guidance and cross-reference to control(s) in Annex A”.

Table 1 *(continued)*

ISO/IEC 27002:2022 Control identifier	ISO/IEC 27002:2022 Control name	Theme
5.29	Information security during disruption	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.30 [a]	ICT readiness for business continuity	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.31	Legal, statutory, regulatory and contractual requirements	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.32	Intellectual property rights	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.33	Protection of records	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.34	Privacy and protection of PII	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.35	Independent review of information security	Public cloud service provider-specific implementation guidance is provided. [b]
5.36	Compliance with policies, rules and standards for information security	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.37	Documented operating procedures	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
Clause 6 – People controls		
6.1	Screening	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
6.2	Terms and conditions of employment	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
6.3	Information security awareness, education and training	Public cloud service provider-specific implementation guidance and other information is provided.[c]
6.4	Disciplinary process	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
6.5	Responsibilities after termination or change of employment	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]

[a] New control introduced in ISO/IEC 27002:2022.

[b] This control is applicable as “Public cloud PII protection implementation guidance”.

[c] This control is applicable as “Public cloud PII protection implementation guidance and other information for public cloud PII protection”.

[d] This control is applicable as “no specific Guidance or other information for Public cloud PII protection”.

[e] This control is applicable as “Public cloud PII protection implementation guidance and cross-reference to control(s) in Annex A”.

Table 1 *(continued)*

ISO/IEC 27002:2022 Control identifier	ISO/IEC 27002:2022 Control name	Theme
6.6	Confidentiality or non-disclosure agreements	Public cloud service provider-specific implementation guidance is provided, together with a cross-reference to control(s) in Annex A. [e]
6.7	Remote working	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
6.8	Information security event reporting	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
Clause 7 – Physical controls		
7.1	Physical security perimeters	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
7.2	Physical entry	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
7.3	Securing offices, rooms and facilities	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
7.4 [a]	Physical security monitoring	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
7.5	Protecting against physical and environmental threats	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
7.6	Working in secure areas	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
7.7	Clear desk and clear screen	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
7.8	Equipment siting and protection	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
7.9	Security of assets off-premises	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
7.10	Storage media	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
7.11	Supporting utilities	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]

[a] New control introduced in ISO/IEC 27002:2022.

[b] This control is applicable as “Public cloud PII protection implementation guidance”.

[c] This control is applicable as “Public cloud PII protection implementation guidance and other information for public cloud PII protection”.

[d] This control is applicable as “no specific Guidance or other information for Public cloud PII protection”.

[e] This control is applicable as “Public cloud PII protection implementation guidance and cross-reference to control(s) in Annex A”.

Table 1 *(continued)*

ISO/IEC 27002:2022 Control identifier	ISO/IEC 27002:2022 Control name	Theme
7.12	Cabling security	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
7.13	Equipment maintenance	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
7.14	Secure disposal or re-use of equipment	Public cloud service provider-specific implementation guidance is provided, together with a cross-reference to control(s) in Annex A. [e]
Clause 8 – Technological controls		
8.1	User endpoint devices	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.2	Privileged access rights	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.3	Information access restriction	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.4	Access to source code	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.5	Secure authentication	Public cloud service provider-specific implementation guidance is provided. [b]
8.6	Capacity management	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.7	Protection against malware	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.8	Management of technical vulnerabilities	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.9 [a]	Configuration management	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.10 [a]	Information deletion	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.11 [a]	Data masking	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]

[a] New control introduced in ISO/IEC 27002:2022.

[b] This control is applicable as "Public cloud PII protection implementation guidance".

[c] This control is applicable as "Public cloud PII protection implementation guidance and other information for public cloud PII protection".

[d] This control is applicable as "no specific Guidance or other information for Public cloud PII protection".

[e] This control is applicable as "Public cloud PII protection implementation guidance and cross-reference to control(s) in Annex A".

Table 1 *(continued)*

ISO/IEC 27002:2022 Control identifier	ISO/IEC 27002:2022 Control name	Theme
8.12 [a]	Data leakage prevention	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.13	Information backup	Public cloud service provider-specific implementation guidance is provided. [b]
8.14	Redundancy of information processing facilities	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.15	Logging	Public cloud service provider-specific implementation guidance is provided, together with a cross-reference to control(s) in Annex A. [e]
8.16 [a]	Monitoring activities	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.17	Clock synchronization	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.18	Use of privileged utility programs	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.19	Installation of software on operational systems	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.20	Networks security	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.21	Security of network services	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.22	Segregation of networks	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.23 [a]	Web filtering	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.24	Use of cryptography	Public cloud service provider-specific implementation guidance is provided. [b]
8.25	Secure development lifecycle	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.26	Application security requirements	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]

[a] New control introduced in ISO/IEC 27002:2022.

[b] This control is applicable as “Public cloud PII protection implementation guidance”.

[c] This control is applicable as “Public cloud PII protection implementation guidance and other information for public cloud PII protection”.

[d] This control is applicable as “no specific Guidance or other information for Public cloud PII protection”.

[e] This control is applicable as “Public cloud PII protection implementation guidance and cross-reference to control(s) in Annex A”.

Table 1 *(continued)*

ISO/IEC 27002:2022 Control identifier	ISO/IEC 27002:2022 Control name	Theme
8.27	Secure system architecture and engineering principles	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.28 [a]	Secure coding	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.29	Security testing in development and acceptance	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.30	Outsourced development	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.31	Separation of development, test and production environments	Public cloud service provider-specific implementation guidance is provided. [b]
8.32	Change management	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.33	Test information	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.34	Protection of information systems during audit testing	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]

[a] New control introduced in ISO/IEC 27002:2022.

[b] This control is applicable as "Public cloud PII protection implementation guidance".

[c] This control is applicable as "Public cloud PII protection implementation guidance and other information for public cloud PII protection".

[d] This control is applicable as "no specific Guidance or other information for Public cloud PII protection".

[e] This control is applicable as "Public cloud PII protection implementation guidance and cross-reference to control(s) in Annex A".

4.2 Control layout

In line with ISO/IEC 27002:2022, the entire set of controls are categorized under the 4 themes found in Table 1 above. Each control has the following elements:

a) Control title: short name of the control;

b) Attribute table: a table shows the value(s) of each attribute for the given control;

c) Control: what the control is;

d) Purpose: why the control should be implemented;

e) Guidance: how the control should be implemented;

f) Other information: explanatory text or references to other related documents.

Subheadings are used in the guidance text for some controls to aid readability where guidance is lengthy and addresses multiple topics. Such headings are not necessarily used in all guidance text.

g) Public cloud PII protection guidance

This provides more detailed information to support the implementation of the control and to meet the control objectives. The guidance should not be considered as entirely suitable or sufficient in all situations and hence will not fulfil the organization's specific control requirements. Alternative or additional controls, or other forms of risk treatment (e.g. avoiding, transferring, or accepting risks), can therefore be appropriate.

h) Other information for public cloud PII protection

This provides further information that is expected to be considered, such as legal considerations and references to other standards.

5 Organizational controls

5.1 Policies for information security

The guidance in ISO/IEC 27002:2022, 5.1 applies. In addition, the following public cloud service provider-specific guidance and associated information also apply.

a) Public cloud PII protection implementation guidance

Contractual agreements should allocate responsibilities between the public cloud PII processor, its sub-contractors and the cloud service customer, taking into account the type of cloud service in question [e.g. a service of an Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or Software as a Service (SaaS) category of the cloud computing reference architecture]. For example, the allocation of responsibility for application layer controls can differ depending on whether the public cloud PII processor is providing a SaaS service or rather is providing a PaaS or IaaS service on which the cloud service customer can build or layer its own applications.

b) Other information for public cloud PII protection

In some jurisdictions, the public cloud PII processor is directly subject to PII protection legislation. In others, PII protection legislation can apply to the PII controller only.

It is necessary that the contract between the cloud service customer and the public cloud PII processor includes a mechanism to ensure the public cloud PII processor supports and manages compliance with the contract between the cloud service customer and the public cloud PII processor. The contract can call for independently audited compliance, acceptable to the cloud service customer, e.g. via the implementation of the relevant controls in this document and in ISO/IEC 27002.

5.2 Information security roles and responsibilities

The guidance in ISO/IEC 27002:2022, 5.2 applies. In addition, the following public cloud service provider-specific guidance also applies.

a) Public cloud PII protection implementation guidance

The public cloud PII processor should have a PII specialist who advises the cloud service customers on the proper handling of PII information.

5.3 Segregation of duties

The guidance in ISO/IEC 27002:2022, 5.3 applies.

5.4 Management responsibilities

The guidance in ISO/IEC 27002:2022, 5.4 applies.

5.5 Contact with authorities

The guidance in ISO/IEC 27002:2022, 5.5 applies.

5.6 Contact with special interest groups

The guidance in ISO/IEC 27002:2022, 5.6 applies.

5.7 Threat intelligence

NOTE New control introduced in ISO/IEC 27002:2022.

The guidance in ISO/IEC 27002:2022, 5.7 applies.

5.8 Information security in project management

The guidance in ISO/IEC 27002:2022, 5.8 applies.

5.9 Inventory of information and other associated assets

The guidance in ISO/IEC 27002:2022, 5.9 applies.

5.10 Acceptable use of information and other associated assets

The guidance in ISO/IEC 27002:2022, 5.10 applies.

5.11 Return of assets

The guidance in ISO/IEC 27002:2022, 5.11 applies.

5.12 Classification of information

The guidance in ISO/IEC 27002:2022, 5.12 applies.

5.13 Labelling of information

The guidance in ISO/IEC 27002:2022, 5.13 applies.

5.14 Information transfer

The guidance in ISO/IEC 27002:2022, 5.14 applies. In addition, the following public cloud service provider-specific guidance also applies.

a) Public cloud PII protection implementation guidance

Whenever physical media are used for information transfer, a system should be put in place to record incoming and outgoing physical media containing PII, including the type of physical media, the authorized sender/recipients, the date and time, and the number of physical media. Where appropriate, cloud service customers should implement, and public cloud PII processors should support technical capacity to apply, additional measures (such as encryption) to reduce the likelihood that unauthorized access could occur en route, prior to arrival at the intended destination. In these cases, both parties can apply their own such measures.

5.15 Access control

The guidance in ISO/IEC 27002:2022, 5.15 applies.

5.16 Identity management

The guidance in ISO/IEC 27002:2022, 5.16 applies. In addition, the following public cloud service provider-specific guidance and associated information also apply.

a) Public cloud PII protection implementation guidance

In the context of the service categories of the cloud computing reference architecture, the cloud service customer can be responsible for some or all aspects of access management for cloud service users under its control. Where appropriate, the public cloud PII processor should enable the cloud service customer to manage the access of cloud service users under the cloud service customer's control.

Procedures for user registration and de-registration should address the situation where user access control is compromised, such as the corruption or compromise of passwords or other user registration data (e.g. as a result of inadvertent disclosure).

NOTE Individual jurisdictions can impose specific requirements regarding the frequency of checks for unused authentication credentials. It is the responsibility of organizations operating in these jurisdictions to ensure that they comply with these requirements.

5.17 Authentication information

The guidance in ISO/IEC 27002:2022, 5.17 applies.

5.18 Access rights

The guidance in ISO/IEC 27002:2022, 5.18 applies.

5.19 Information security in supplier relationships

The guidance in ISO/IEC 27002:2022, 5.19 applies.

5.20 Addressing information security within supplier agreements

The guidance in ISO/IEC 27002:2022, 5.20 applies.

5.21 Managing information security in the ICT supply chain

The guidance in ISO/IEC 27002:2022, 5.21 applies.

5.22 Monitoring, review and change management of supplier services

The guidance in ISO/IEC 27002:2022, 5.22 applies.

5.23 Information security for use of cloud services

NOTE New control introduced in ISO/IEC 27002:2022.

The guidance in ISO/IEC 27002:2022, 5.23 applies.

5.24 Information security incident management planning and preparation

The guidance in ISO/IEC 27002:2022, 5.24 applies.

5.25 Assessment and decision on information security events

The guidance in ISO/IEC 27002:2022, 5.25 applies.

5.26 Response to information security incidents

The guidance in ISO/IEC 27002:2022, 5.26 applies.

a) Public cloud PII protection implementation guidance

An information security incident should trigger a review by the public cloud PII processor, as part of its information security incident management process, to determine if a data breach involving PII has taken place (see A.10.1).

Not all information security events should necessarily trigger such a review. It is possible that an information security event does not result in actual, or the significant probability of, unauthorized access to PII or to any of the public cloud PII processor's equipment or facilities storing PII, and can include, without limitation, pings and other diagnostic probes to firewalls or edge servers.

5.27 Learning from information security incidents

The guidance in ISO/IEC 27002:2022, 5.27 applies.

5.28 Collection of evidence

The guidance in ISO/IEC 27002:2022, 5.28 applies.

5.29 Information security during disruption

The guidance in ISO/IEC 27002:2022, 5.29 applies.

5.30 ICT readiness for business continuity

NOTE New control introduced in ISO/IEC 27002:2022.

The guidance in ISO/IEC 27002:2022, 5.30 applies.

5.31 Legal, statutory, regulatory and contractual requirements

The guidance in ISO/IEC 27002:2022, 5.31 applies.

5.32 Intellectual property rights

The guidance in ISO/IEC 27002:2022, 5.32 applies.

5.33 Protection of records

The guidance in ISO/IEC 27002:2022, 5.33 applies.

5.34 Privacy and protection of PII

The guidance in ISO/IEC 27002:2022, 5.34 applies.

5.35 Independent review of information security

The guidance in ISO/IEC 27002:2022, 5.35 applies. In addition, the following public cloud service provider-specific guidance also applies.

a) Public cloud PII protection implementation guidance

In cases where individual cloud service customer audits are impractical or can increase risks to security, the public cloud PII processor should make available to prospective cloud service customers, prior to entering into, and for the duration of, a contract, independent evidence that information security is implemented and

operated according to the public cloud PII processor's policies and procedures. A relevant independent audit as selected by the public cloud PII processor should normally be an acceptable method for fulfilling the cloud service customer's interest in reviewing the public cloud PII processor's processing operations, provided sufficient transparency is provided.

5.36 Compliance with policies, rules and standards for information security

The guidance in ISO/IEC 27002:2022, 5.36 applies.

5.37 Documented operating procedures

The guidance in ISO/IEC 27002:2022, 5.37 applies.

6 People controls

6.1 Screening

The guidance in ISO/IEC 27002:2022, 6.1 applies.

6.2 Terms and conditions of employment

The guidance in ISO/IEC 27002:2022, 6.2 applies.

6.3 Information security awareness, education and training

The guidance in ISO/IEC 27002:2022, 6.3 applies. In addition, the following public cloud service provider-specific guidance and associated information also apply.

a) Public cloud PII protection implementation guidance

Measures should be put in place to make relevant staff aware of the possible consequences on the public cloud PII processor (e.g. loss of business and brand or reputational damage), on the staff member (e.g. disciplinary consequences) and on the PII principal (e.g. physical, material and emotional consequences) of breaching privacy or security rules and procedures, especially those addressing the handling of PII.

b) Other information for public cloud PII protection

In some jurisdictions, the public cloud PII processor can be subject to legal sanctions, including substantial fines directly from the local PII protection authority.

6.4 Disciplinary process

The guidance in ISO/IEC 27002:2022, 6.4 applies.

6.5 Responsibilities after termination or change of employment

The guidance in ISO/IEC 27002:2022, 6.5 applies.

6.6 Confidentiality or non-disclosure agreements

NOTE Additional controls and guidance relevant to confidentiality or non-disclosure agreements can be found in A.10.1.

The guidance in ISO/IEC 27002:2022, 6.6 applies.

6.7 Remote working

The guidance in ISO/IEC 27002:2022, 6.7 applies.

6.8 Information security event reporting

The guidance in ISO/IEC 27002:2022, 6.8 applies.

7 Physical controls

7.1 Physical security perimeters

The guidance in ISO/IEC 27002:2022, 7.1 applies.

7.2 Physical entry

The guidance in ISO/IEC 27002:2022, 7.2 applies.

7.3 Securing offices, rooms and facilities

The guidance in ISO/IEC 27002:2022, 7.3 applies.

7.4 Physical security monitoring

NOTE New control introduced in ISO/IEC 27002:2022.

The guidance in ISO/IEC 27002:2022, 7.4 applies.

7.5 Protecting against physical and environmental threats

The guidance in ISO/IEC 27002:2022, 7.5 applies.

7.6 Working in secure areas

The guidance in ISO/IEC 27002:2022, 7.6 applies.

7.7 Clear desk and clear screen

The guidance in ISO/IEC 27002:2022, 7.7 applies.

7.8 Equipment siting and protection

The guidance in ISO/IEC 27002:2022, 7.8 applies.

7.9 Security of assets off-premises

The guidance in ISO/IEC 27002:2022, 7.9 applies.

7.10 Storage media

The guidance in ISO/IEC 27002:2022, 7.10 applies.

7.11 Supporting utilities

The guidance in ISO/IEC 27002:2022, 7.11 applies.

7.12 Cabling security

The guidance in ISO/IEC 27002:2022, 7.12 applies.

7.13 Equipment maintenance

The guidance in ISO/IEC 27002:2022, 7.13 applies.

7.14 Secure disposal or re-use of equipment

The guidance in ISO/IEC 27002:2022, 7.14 applies. The following public cloud service provider-specific guidance also applies.

a) Public cloud PII protection implementation guidance

For the purposes of secure disposal or re-use, equipment containing storage media that can possibly contain PII should be treated as though it does.

NOTE Additional controls and guidance relevant to secure disposal or re-use of equipment can be found in A.11.7.

8 Technological controls

8.1 User endpoint devices

The guidance in ISO/IEC 27002:2022, 8.1 applies.

8.2 Privileged access rights

The guidance in ISO/IEC 27002:2022, 8.2 applies.

8.3 Information access restriction

The guidance in ISO/IEC 27002:2022, 8.3 applies.

8.4 Access to source code

The guidance in ISO/IEC 27002:2022, 8.4 applies.

8.5 Secure authentication

The guidance in ISO/IEC 27002:2022, 8.5 applies. The following public cloud service provider-specific guidance also applies.

a) Public cloud PII protection implementation guidance

Where required, the public cloud PII processor should provide secure log-on procedures for any accounts requested by the cloud service customer for cloud service users under its control.

8.6 Capacity management

The guidance in ISO/IEC 27002:2022, 8.6 applies.

8.7 Protection against malware

The guidance in ISO/IEC 27002:2022, 8.7 applies.

8.8 Management of technical vulnerabilities

The guidance in ISO/IEC 27002:2022, 8.8 applies.

8.9 Configuration management

NOTE New control introduced in ISO/IEC 27002:2022.

The guidance in ISO/IEC 27002:2022, 8.9 applies.

8.10 Information deletion

NOTE New control introduced in ISO/IEC 27002:2022.

The guidance in ISO/IEC 27002:2022, 8.10 applies.

8.11 Data masking

NOTE New control introduced in ISO/IEC 27002:2022.

The guidance in ISO/IEC 27002:2022, 8.11 applies.

8.12 Data leakage prevention

NOTE New control introduced in ISO/IEC 27002:2022.

The guidance in ISO/IEC 27002:2022, 8.12 applies.

8.13 Information backup

The guidance in ISO/IEC 27002:2022, 8.13 applies. The following public cloud service provider-specific guidance also applies.

a) Public cloud PII protection implementation guidance

Information processing systems based on the cloud computing model introduce additional or alternative mechanisms to off-site backups for protecting against loss of data, ensuring continuity of data processing operations, and providing the ability to restore data processing operations after a disruptive event. Multiple copies of data in either physically or logically diverse locations or both (which can be within the information processing system itself) should be created or maintained for the purposes of either backup or recovery or both.

PII-specific responsibilities in this respect can lie with the cloud service customer. Where the public cloud PII processor explicitly provides backup and restore services to the cloud service customer, the public cloud PII processor should provide information to the cloud service customer about the capabilities of the cloud service with respect to backup and restoration of the cloud service customer data.

Procedures should be put in place to allow for restoration of data processing operations within a specified, documented period after a disruptive event.

The back-up and recovery procedures should be reviewed at a specified, documented frequency.

NOTE Some jurisdictions can impose specific requirements regarding the frequency of reviews of backup and recovery procedures. It is the responsibility of organizations operating in these jurisdictions to ensure that they comply with these requirements.

The use of sub-contractors to store replicated or backup copies of data being processed is covered by the controls A.8.1 and A.11.12 in this document applying to sub-contracted PII processing. Where physical media transfers take place this is also covered by controls 5.14 and A.11.5 in this document.

The public cloud PII processor should have a policy which addresses the requirements for the backup of information and any further requirements (e.g. contractual requirements) for the erasure of PII contained in information held for backup purposes.

8.14 Redundancy of information processing facilities

The guidance in ISO/IEC 27002:2022, 8.14 applies.

8.15 Logging

The guidance in ISO/IEC 27002:2022, 8.15 applies. The following public cloud service provider-specific guidance also applies.

a) Public cloud PII protection implementation guidance

A process should be put in place to review event logs with a specified, documented periodicity, to identify irregularities and propose remediation efforts.

Where possible, event logs should record whether or not PII has been changed (e.g. added, modified or deleted) as a result of an event and by whom. Where multiple service providers are involved in providing service from different service categories of the cloud computing reference architecture, there can be varied or shared roles in implementing this guidance.

The public cloud PII processor should define criteria regarding if, when and how log information can be made available to or usable by the cloud service customer. These procedures should be made available to the cloud service customer.

Where a cloud service customer is permitted to access log records controlled by the public cloud PII processor, the public cloud PII processor should ensure that the cloud service customer can only access records that relate to that cloud service customer's activities, and cannot access any log records which relate to the activities of other cloud service customers.

Log information recorded for purposes such as security monitoring and operational diagnostics can contain PII. Measures, such as controlling access, should be put in place to ensure that logged information is only used for its intended purposes.

A procedure, preferably automatic, should be put in place to ensure that logged information is deleted within a specified and documented period.

8.16 Monitoring activities

NOTE New control introduced in ISO/IEC 27002:2022.

The guidance in ISO/IEC 27002:2022, 8.16 applies.

8.17 Clock synchronization

The guidance in ISO/IEC 27002:2022, 8.17 applies.

8.18 Use of privileged utility programs

The guidance in ISO/IEC 27002:2022, 8.18 applies.

8.19 Installation of software on operational systems

The guidance in ISO/IEC 27002:2022, 8.19 applies.

8.20 Networks security

The guidance in ISO/IEC 27002:2022, 8.20 applies.

8.21 Security of network services

The guidance in ISO/IEC 27002:2022, 8.21 applies.

8.22 Segregation of networks

The guidance in ISO/IEC 27002:2022, 8.22 applies.

8.23 Web filtering

NOTE New control introduced in ISO/IEC 27002:2022.

The guidance in ISO/IEC 27002:2022, 8.23 applies.

8.24 Use of cryptography

The guidance in ISO/IEC 27002:2022, 8.24 applies. The following public cloud service provider-specific guidance also applies.

a) Public cloud PII protection implementation guidance

The public cloud PII processor should also provide information to the cloud service customer about any capabilities it provides that can assist the cloud service customer in applying and managing its own cryptographic protection and processes such as various methods to manage keys or secrets in a vault, key management system (KMS), hardware security module (HSM) backed service, cloud HSM, etc.

NOTE In some jurisdictions, it can be required to apply cryptography to protect particular kinds of PII, such as health data concerning a PII principal, resident registration numbers, passport numbers and driver's licence numbers.

8.25 Secure development lifecycle

The guidance in ISO/IEC 27002:2022, 8.25 applies.

8.26 Application security requirements

The guidance in ISO/IEC 27002:2022, 8.26 applies.

8.27 Secure system architecture and engineering principles

The guidance in ISO/IEC 27002:2022, 8.27 applies.

8.28 Secure coding

NOTE New control introduced in ISO/IEC 27002:2022.

The guidance in ISO/IEC 27002:2022, 8.28 applies.

8.29 Security testing in development and acceptance

The guidance in ISO/IEC 27002:2022, 8.29 applies.

8.30 Outsourced development

The guidance in ISO/IEC 27002:2022, 8.30 applies.

8.31 Separation of development, test and production environments

The guidance in ISO/IEC 27002:2022, 8.31 applies. The following public cloud service provider-specific guidance also applies.

a) Public cloud PII protection implementation guidance

Where the use of PII for testing purposes cannot be avoided, a risk assessment should be undertaken. Technical and organizational measures should be implemented to minimize the risks identified.

8.32 Change management

The guidance in ISO/IEC 27002:2022, 8.32 applies.

8.33 Test information

The guidance in ISO/IEC 27002:2022, 8.33 applies.

8.34 Protection of information systems during audit testing

The guidance in ISO/IEC 27002:2022, 8.34 applies.

Annex A
(informative)

Public cloud PII processor extended control set for PII protection

A.1 General

This annex specifies new controls and associated implementation guidance which, in combination with the controls and guidance in ISO/IEC 27002 (see Clauses 5 to 8), make up an extended control set to meet the requirements for PII protection which apply to public cloud service providers acting as PII processors.

These additional controls are classified according to the 11 privacy principles of ISO/IEC 29100. In many cases, the controls can be classified under more than one of the privacy principles. In such cases, they are classified under the most relevant principle.

A.2 Consent and choice

A.2.1 Obligation to co-operate regarding PII principals' rights

a) Control

The public cloud PII processor should enable the cloud service customer to fulfil their obligations, by providing them with the means to facilitate the exercise of the PII principals' rights to access, correct and erase PII pertaining to them.

b) Public cloud PII protection implementation guidance

The PII controller's obligations in this respect can be defined by law, by regulations or by contract. These obligations can include matters where the cloud service customer uses the services of the public cloud PII processor for implementation. For example, this can include the correction or deletion of PII in a timely fashion.

Where the PII controller depends on the public cloud PII processor for information or technical measures to facilitate the exercise of PII principals' rights, the relevant information or technical measures should be specified in the contract.

A.3 Purpose legitimacy and specification

A.3.1 Public cloud PII processor's purpose

a) Control

PII to be processed under a contract should not be processed for any purpose independent of the instructions of the cloud service customer.

b) Public cloud PII protection implementation guidance

Instructions can be contained in the contract between the public cloud PII processor and the cloud service customer including, e.g. the objective and time frame to be achieved by the service.

In order to achieve the cloud service customer's purpose, there can be technical reasons why it is appropriate for a public cloud PII processor to determine the method for PII processing, consistent with the general instructions of the cloud service customer but without the cloud service customer's express instruction. For example, in order to efficiently utilize network or processing capacity it can be necessary to allocate specific

processing resources depending on certain characteristics of the PII principal. In circumstances where the public cloud PII processor's determination of the processing method involves the collection and use of PII, the public cloud PII processor should adhere to the relevant privacy principles set forth in ISO/IEC 29100 and the principles of "privacy by design" (see References [64] and [65]).

The public cloud PII processor should provide the cloud service customer with all relevant information, in a timely fashion, to allow the cloud service customer to ensure the public cloud PII processor's compliance with purpose specification and limitation principles and ensure that no PII is processed by the public cloud PII processor or any of its sub-contractors for further purposes independent of the instructions of the cloud service customer.

A.3.2 Public cloud PII processor's commercial use

a) Control

PII processed under a contract should not be used by the public cloud PII processor for the purposes of marketing and advertising without express consent. Such consent should not be a condition of receiving the service.

NOTE This control is an addition to the more general control in A.3.1 and does not replace or otherwise supersede it.

A.4 Collection limitation

No additional controls are relevant to this privacy principle.

A.5 Data minimization

A.5.1 Secure erasure of temporary files

a) Control

Temporary files and documents should be erased or destroyed within a specified, documented period.

b) Public cloud PII protection implementation guidance

Implementation guidance on PII erasure is provided in A.10.3.

Information systems can create temporary files in the normal course of their operation. Such files are specific to the system or application, but can include file system roll-back journals and temporary files associated with the updating of databases and the operation of other application software. Temporary files are not needed after the related information processing task has completed and should be deleted after completion unless the particular circumstances require that they should not be deleted. The length of time for which these files remain in use is not always deterministic but a "garbage collection" procedure should identify the relevant files and determine how long it has been since they were last used.

PII processing information systems should implement a periodic check that unused temporary files above a specified age are deleted.

A.6 Use, retention and disclosure limitation

A.6.1 PII disclosure notification

a) Control

It is expected that the contract between the public cloud PII processor and the cloud service customer requires the public cloud PII processor to notify the cloud service customer, according to any procedure and

time periods agreed in the contract, of any legally binding request for disclosure of PII by a law enforcement authority, unless such a disclosure is otherwise prohibited.

b) Public cloud PII protection implementation guidance

The public cloud PII processor should provide contractual guarantees that it will:

— reject any requests for PII disclosure that are not legally binding;

— consult the corresponding cloud service customer, where legally permissible, before making any PII disclosure; and

— accept any contractually agreed requests for PII disclosures that are authorized by the corresponding cloud service customer.

EXAMPLE A possible prohibition on disclosure would be a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

A.6.2 Recording of PII disclosures

a) Control

Disclosure of PII to third parties should be recorded, including what PII has been disclosed, the reason for disclosing the PII, to whom and at what time.

b) Public cloud PII protection implementation guidance

PII can be disclosed during the course of normal operations. These disclosures should be recorded. Any additional disclosures to third parties, such as those arising from lawful investigations or external audits, should also be recorded. The records should include the source of the disclosure, reason for disclosure and the source of the authority to make the disclosure.

A.7 Accuracy and quality

No additional controls are relevant to this privacy principle.

A.8 Openness, transparency and notice

A.8.1 Disclosure of sub-contracted PII processing

a) Control

If public cloud PII processors intend to use sub-contractors to process PII, this should be disclosed to the relevant cloud service customers in advance.

b) Public cloud PII protection implementation guidance

Provisions for the use of sub-contractors to process PII should be transparent in the contract between the public cloud PII processor and the cloud service customer. The contract should specify that sub-contractors can only be commissioned on the basis of a consent that can generally be given by the cloud service customer at the beginning of the service. The public cloud PII processor should inform the cloud service customer in a timely fashion of any intended changes in this regard so that the cloud service customer has the ability to object to such changes or to terminate the contract.

Information disclosed should cover the fact that sub-contracting is used and the names of relevant sub-contractors, but not any business-specific details. The information disclosed should also include the countries in which sub-contractors can process data (see A.12.1) and the means by which sub-contractors are obliged to meet or exceed the obligations of the public cloud PII processor (see A.11.12).

Where public disclosure of sub-contractor information is assessed as leading to security risk increase, disclosure should be made under a non-disclosure agreement and/or on the request of the cloud service customer. The cloud service customer should be made aware that the information is available.

A.9 Individual participation and access

No additional controls are relevant to this privacy principle.

A.10 Accountability

A.10.1 Notification of a data breach involving PII

a) Control

The public cloud PII processor should promptly notify the relevant cloud service customer in the event of any unauthorized access to PII or unauthorized access to processing equipment or facilities resulting in loss, disclosure or alteration of PII.

b) Public cloud PII protection implementation guidance

Provisions covering the notification of a data breach involving PII should form part of the contract between the public cloud PII processor and the cloud service customer. The contract should specify how the public cloud PII processor will provide the information necessary for the cloud service customer to fulfil his obligation to notify relevant authorities. This notification obligation does not extend to a data breach caused by the cloud service customer or PII principal, or within system components for which they are responsible. The contract should also define the maximum delay in notification of a data breach involving PII.

In the event that a data breach involving PII has occurred, a record should be maintained with a description of the incident, the time period, the consequences of the incident, the name of the reporter, to whom the incident was reported, the steps taken to resolve the incident (including the person in charge and the data recovered) and the fact that the incident resulted in loss, disclosure or alteration of PII.

In the event that a data breach involving PII has occurred, the record should also include a description of the data compromised, if known. If notifications were performed, the record should include the steps taken to notify either the cloud service customer or regulatory authorities or both.

In some jurisdictions, relevant legislation or regulations can require the public cloud PII processor to directly notify appropriate regulatory authorities (e.g. a PII protection authority) of a data breach involving PII.

NOTE There can be other breaches requiring notification that are not covered here, e.g. collection without consent or other authorization, use for unauthorized purposes, etc.

A.10.2 Retention period for administrative security policies and guidelines

a) Control

The existing copies of security policies and operating procedures that are updated should be retained for a specified, documented period of replacement.

b) Public cloud PII protection implementation guidance

Review of current and historical policies and procedures can be required, e.g. in the cases of customer dispute resolution and investigation by a PII protection authority. A minimum retention period of five years is recommended in the absence of a specific contractual requirement or other requirements as applicable.

A.10.3 PII return, transfer and disposal

a) Control

The public cloud PII processor should have a policy in respect of these activities and should make this policy available to the cloud service customer.

b) Public cloud PII protection implementation guidance

At some point in time, PII are expected to be disposed of in some manner. This can involve returning the PII to the cloud service customer, transferring it to another public cloud PII processor or to a PII controller (e.g. as a result of a merger), securely deleting or otherwise destroying it, anonymizing it or archiving it.

The public cloud PII processor should provide the information necessary to allow the cloud service customer to ensure that PII processed under a contract is erased (by the public cloud PII processor and any of its sub-contractors) from wherever they are stored, including for the purposes of backup and business continuity, as soon as they are no longer necessary for the specific purposes of the cloud service customer. The nature of the disposition mechanisms (de-linking, overwriting, demagnetization, destruction or other forms of erasure) and/or the applicable commercial standards should be provided for contractually.

The public cloud PII processor should develop and implement a policy in respect of the disposition of PII and should make this policy available to the cloud service customer.

The policy should cover the retention period for PII before its destruction after termination of a contract, to protect the cloud service customer from losing PII through an accidental lapse of the contract.

NOTE This control and guidance is also relevant under the retention element of the "Use, retention and disclosure limitation" principle (see A.6).

A.11 Information security

A.11.1 Confidentiality or non-disclosure agreements

a) Control

Individuals under the public cloud PII processor's control with access to PII should be subject to a confidentiality obligation.

b) Public cloud PII protection implementation guidance

A confidentiality agreement, in whatever form, between the public cloud PII processor, its employees and its agents should ensure that employees and agents do not disclose PII for purposes independent of the instructions of the cloud service customer (see A.3.1). The obligations of the confidentiality agreement should survive termination of any relevant contract.

A.11.2 Restriction of the creation of hardcopy material

a) Control

The creation of hardcopy material displaying PII should be restricted.

b) Public cloud PII protection implementation guidance

Hardcopy material includes material created by printing.

A.11.3 Control and logging of data restoration

a) Control

There should be a procedure for, and a log of, data restoration efforts.

b) Public cloud PII protection implementation guidance

The log of data restoration efforts should contain: the person responsible, a description of the restored data, and the data that were restored manually.

A.11.4 Protecting data on storage media leaving the premises

a) Control

PII on media leaving the organization's premises should be subject to an authorization procedure and should not be accessible to anyone other than authorized personnel (e.g. by encrypting the data concerned).

A.11.5 Use of unencrypted portable storage media and devices

a) Control

Portable physical media and portable devices that do not permit encryption should not be used except where it is unavoidable, and any use of such portable media and devices should be documented.

A.11.6 Encryption of PII transmitted over public data-transmission networks

a) Control

PII that is transmitted over public data-transmission networks should be encrypted prior to transmission.

b) Public cloud PII protection implementation guidance

In some cases, e.g. the exchange of e-mail, the inherent characteristics of public data-transmission network systems can require that some header or traffic data be exposed for effective transmission.

Where multiple service providers are involved in providing service from different service categories of the cloud computing reference architecture, there can be varied or shared roles in implementing this guidance.

A.11.7 Secure disposal of hardcopy materials

a) Control

Where hardcopy materials are destroyed, they should be destroyed securely using mechanisms such as cross-cutting, shredding, incinerating, pulping, etc.

A.11.8 Unique use of user IDs

a) Control

If more than one individual has access to stored PII, then they should each have a distinct user ID for identification, authentication and authorization purposes.

A.11.9 User ID management

a) Control

De-activated or expired user IDs should not be granted to other individuals.

b) Public cloud PII protection implementation guidance

In the context of the whole cloud computing reference architecture, the cloud service customer can be responsible for some or all aspects of user ID management for cloud service users under its control.

A.11.10 Records of authorized users

a) Control

An up-to-date record of the users or profiles of users who have authorized access to the information system should be maintained.

b) Public cloud PII protection implementation guidance

A user profile should be maintained for all users whose access is authorized by the public cloud PII processor. The profile of a user comprises the set of data about that user, including user ID, which is necessary to implement the technical controls providing authorized access to the information system.

A.11.11 Contract measures

a) Control

Contracts between the cloud service customer and the public cloud PII processor should specify minimum technical and organizational measures to ensure that the contracted security arrangements are in place and that data are not processed for any purpose independent of the instructions of the controller. Such measures should not be subject to unilateral reduction by the public cloud PII processor.

b) Public cloud PII protection implementation guidance

Information security and PII protection obligations relevant to the public cloud PII processor can arise directly from applicable law. Where this is not the case, PII protection obligations relevant to the public cloud PII processor are expected to be covered in the contract.

The controls in this document, together with the controls in ISO/IEC 27002, are intended as a reference catalogue of measures to assist in entering into an information processing contract in respect of PII. The public cloud PII processor should inform a prospective cloud service customer, before entering into a contract, about the information security and privacy controls implemented for the protection of PII.

The public cloud PII processor should be transparent about its capabilities during the process of entering into a contract. However, it is ultimately the cloud service customer's responsibility to ensure that the measures implemented by the public cloud PII processor meet its obligations.

A.11.12 Sub-contracted PII processing

a) Control

Contracts between the public cloud PII processor and any sub-contractors that process PII should specify minimum technical and organizational measures that meet the information security and PII protection obligations of the public cloud PII processor. Such measures should not be subject to unilateral reduction by the sub-contractor.

b) Public cloud PII protection implementation guidance

The use of sub-contractors to store backup copies is covered by this control (see A.8.1).

A.11.13 Access to data on pre-used data storage space

a) Control

The public cloud PII processor should ensure that whenever data storage space is assigned to a cloud service customer, any data previously residing on that storage space is not visible to that cloud service customer.

b) Public cloud PII protection implementation guidance

On deletion by a cloud service user of data held in an information system, performance issues can mean that explicit erasure of those data are impractical. This creates the risk that another user can read the data. Such risk should be avoided by specific technical measures.

No specific guidance is especially appropriate for dealing with all cases in implementing this control. However, as an example, some cloud infrastructure, platforms or applications will return either zeroes or nonces if a cloud service user attempts to read storage space which has not been overwritten by that user's own data.

A.12 Privacy compliance

A.12.1 Geographical location of PII

a) Control

The public cloud PII processor should specify and document the countries in which PII can possibly be stored.

b) Public cloud PII protection implementation guidance

The identities of the countries where PII can possibly be stored should be made available to cloud service customers. The identities of the countries arising from the use of sub-contracted PII processing should be included. Where specific contractual agreements apply to the international transfer of data, such as model contract clauses, binding corporate rules or cross border privacy rules, the agreements and the countries or circumstances in which such agreements apply should also be identified. The public cloud PII processor should inform the cloud service customer in a timely fashion of any intended changes in this regard so that the cloud service customer has the ability to object to such changes or to terminate the contract.

A.12.2 Intended destination of PII

a) Control

PII transmitted using a data-transmission network should be subject to appropriate controls designed to ensure that data reaches its intended destination.

Annex B
(informative)

Correspondence between this document and the first edition ISO/IEC 27018:2019

The purpose of this annex is to provide backwards compatibility with the first edition of this document (ISO/IEC 27018:2019) for organizations currently using it and wanting 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 27018:2019.

Table B.1 — Correspondence between controls in this document and controls in ISO/IEC 27018:2019

ISO/IEC 27018:2025 control identifier	ISO/IEC 27018:2019 control identifier	Control name
5.1	05.1.1, 05.1.2	Policies for information security
5.2	06.1.1	Information security roles and responsibilities
5.3	06.1.2	Segregation of duties
5.4	07.2.1	Management responsibilities
5.5	06.1.3	Contact with authorities
5.6	06.1.4	Contact with special interest groups
5.7	New	Threat intelligence
5.8	06.1.5, 14.1.1	Information security in project management
5.9	08.1.1, 08.1.2	Inventory of information and other associated assets
5.10	08.1.3, 08.2.3	Acceptable use of information and other associated assets
5.11	08.1.4	Return of assets
5.12	08.2.1	Classification of information
5.13	08.2.2	Labelling of information
5.14	13.2.1, 13.2.2, 13.2.3	Information transfer
5.15	09.1.1, 09.1.2	Access control
5.16	09.2.1	Identity management
5.17	09.2.4, 09.3.1, 09.4.3	Authentication information
5.18	09.2.2, 09.2.5, 09.2.6	Access rights
5.19	15.1.1	Information security in supplier relationships
5.20	15.1.2	Addressing information security within supplier agreements
5.21	15.1.3	Managing information security in the ICT supply chain
5.22	15.2.1, 15.2.2	Monitoring, review and change management of supplier services
5.23	New	Information security for use of cloud services
5.24	16.1.1	Information security incident management planning and preparation
5.25	16.1.4	Assessment and decision on information security events
5.26	16.1.5	Response to information security incidents

Table B.1 *(continued)*

ISO/IEC 27018:2025 control identifier	ISO/IEC 27018:2019 control identifier	Control name
5.27	16.1.6	Learning from information security incidents
5.28	16.1.7	Collection of evidence
5.29	17.1.1, 17.1.2, 17.1.3	Information security during disruption
5.30	New	ICT readiness for business continuity
5.31	18.1.1, 18.1.5	Legal, statutory, regulatory and contractual requirements
5.32	18.1.2	Intellectual property rights
5.33	18.1.3	Protection of records
5.34	18.1.4	Privacy and protection of PII
5.35	18.2.1	Independent review of information security
5.36	18.2.2, 18.2.3	Compliance with policies, rules and standards for information security
5.37	12.1.1	Documented operating procedures
6.1	07.1.1	Screening
6.2	07.1.2	Terms and conditions of employment
6.3	07.2.2	Information security awareness, education and training
6.4	07.2.3	Disciplinary process
6.5	07.3.1	Responsibilities after termination or change of employment
6.6	13.2.4	Confidentiality or non-disclosure agreements
6.7	06.2.2	Remote working
6.8	16.1.2, 16.1.3	Information security event reporting
7.1	11.1.1	Physical security perimeters
7.2	11.1.2, 11.1.6	Physical entry
7.3	11.1.3	Securing offices, rooms and facilities
7.4	New	Physical security monitoring
7.5	11.1.4	Protecting against physical and environmental threats
7.6	11.1.5	Working in secure areas
7.7	11.2.9	Clear desk and clear screen
7.8	11.2.1	Equipment siting and protection
7.9	11.2.6	Security of assets off-premises
7.10	08.3.1, 08.3.2, 08.3.3, 11.2.5	Storage media
7.11	11.2.2	Supporting utilities
7.12	11.2.3	Cabling security
7.13	11.2.4	Equipment maintenance
7.14	11.2.7	Secure disposal or re-use of equipment
8.1	06.2.1, 11.2.8	User endpoint devices
8.2	09.2.3	Privileged access rights
8.3	09.4.1	Information access restriction
8.4	09.4.5	Access to source code
8.5	09.4.2	Secure authentication
8.6	12.1.3	Capacity management
8.7	12.2.1	Protection against malware
8.8	12.6.1, 18.2.3	Management of technical vulnerabilities

Table B.1 *(continued)*

ISO/IEC 27018:2025 control identifier	ISO/IEC 27018:2019 control identifier	Control name
8.9	New	Configuration management
8.10	New	Information deletion
8.11	New	Data masking
8.12	New	Data leakage prevention
8.13	12.3.1	Information backup
8.14	17.2.1	Redundancy of information processing facilities
8.15	12.4.1, 12.4.2, 12.4.3	Logging
8.16	New	Monitoring activities
8.17	12.4.4	Clock synchronization
8.18	09.4.4	Use of privileged utility programs
8.19	12.5.1, 12.6.2	Installation of software on operational systems
8.20	13.1.1	Networks security
8.21	13.1.2	Security of network services
8.22	13.1.3	Segregation of networks
8.23	New	Web filtering
8.24	10.1.1, 10.1.2	Use of cryptography
8.25	14.2.1	Secure development lifecycle
8.26	14.1.2, 14.1.3	Application security requirements
8.27	14.2.5	Secure system architecture and engineering principles
8.28	New	Secure coding
8.29	14.2.8, 14.2.9	Security testing in development and acceptance
8.30	14.2.7	Outsourced development
8.31	12.1.4, 14.2.6	Separation of development, test and production environments
8.32	12.1.2, 14.2.2, 14.2.3, 14.2.4	Change management
8.33	14.3.1	Test information
8.34	12.7.1	Protection of information systems during audit testing

Bibliography

[1] ISO 9000, *Quality management systems — Fundamentals and vocabulary*

[2] ISO 55001, *Asset management — Asset management system — Requirements*

[3] ISO/IEC 11770 (all parts), *Information security — Key management*

[4] ISO/IEC 15408 (all parts), *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security*

[5] ISO 15489 (all parts), *Information and documentation — Records management*

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

[7] ISO/IEC 22123-2, *Information technology — Cloud computing — Part 2: Concepts*

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

[9] ISO/IEC 19086 (all parts), *Cloud computing — Service level agreement (SLA) framework*

[10] ISO/IEC 19770 (all parts), *Information technology — IT asset management*

[11] ISO/IEC 19941, *Information technology — Cloud computing — Interoperability and portability*

[12] ISO/IEC 20889, *Privacy enhancing data de-identification terminology and classification of techniques*

[13] ISO 21500, *Project, programme and portfolio management — Context and concepts*

[14] ISO 21502, *Project, programme and portfolio management — Guidance on project management*

[15] ISO 22301, *Security and resilience — Business continuity management systems — Requirements*

[16] ISO 22313, *Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301*

[17] ISO/TS 22317, *Security and resilience — Business continuity management systems — Guidelines for business impact analysis*

[18] ISO 22396, *Security and resilience — Community resilience — Guidelines for information exchange between organizations*

[19] ISO/IEC/TS 23167, *Information technology — Cloud computing — Common technologies and techniques*

[20] ISO/IEC 23751, *Information technology — Cloud computing and distributed platforms — Data sharing agreement (DSA) framework*

[21] ISO/IEC 24760 (all parts), *IT Security and Privacy — A framework for identity management*

[22] ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*

[23] ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*[1)]

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

[25] ISO/IEC 27007, *Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing*

1) Cancelled and replaced by ISO/IEC 27002:2022.

[26] ISO/IEC/TS 27008, *Information technology — Security techniques — Guidelines for the assessment of information security controls*

[27] ISO/IEC 27011, *Information security, cybersecurity and privacy protection — Information security controls based on ISO/IEC 27002 for telecommunications organizations*

[28] ISO/IEC/TR 27016, *Information technology — Security techniques — Information security management — Organizational economics*

[29] ISO/IEC 27017, *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*

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

[31] ISO/IEC 27019, *Information security, cybersecurity and privacy protection — Information security controls for the energy utility industry*

[32] ISO/IEC 27031, *Cybersecurity — Information and communication technology readiness for business continuity*

[33] ISO/IEC 27033 (all parts), *— Information technology – Network security*

[34] ISO/IEC 27034 (all parts), *Information technology — Application security*

[35] ISO/IEC 27035-1, *Information technology — Information security incident management — Part 1: Principles and process*

[36] ISO/IEC 27035-2, *Information technology — Information security incident management — Part 2: Guidelines to plan and prepare for incident response*

[37] ISO/IEC 27036 (all parts), *Cybersecurity — Supplier relationships*

[38] ISO/IEC 27037, *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*

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

[40] ISO/IEC 27050 (all parts), *Information technology — Electronic discovery*

[41] ISO/IEC/TS 27110, *Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines*

[42] ISO/IEC 27701, *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*

[43] ISO 27799, *Health informatics — Information security management in health using ISO/IEC 27002*

[44] ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

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

[46] ISO/IEC 29134, *Information technology — Security techniques — Guidelines for privacy impact assessment*

[47] ISO/IEC 29146, *Information technology — Security techniques — A framework for access management*

[48] ISO/IEC 29147, *Information technology — Security techniques — Vulnerability disclosure*

[49] ISO 30000, *Ships and marine technology — Ship recycling management systems — Specifications for management systems for safe and environmentally sound ship recycling facilities*

[50] ISO/IEC 30111, *Information technology — Security techniques — Vulnerability handling processes*

[51] ISO 31000:2018, *Risk management — Guidelines*

[52] IEC 31010, *Risk management — Risk assessment techniques*

[53] ISO/IEC 22123 (all parts), *Information technology — Cloud computing*

[54] ISO/IEC 27555, *Information security, cybersecurity and privacy protection — Guidelines on personally identifiable information deletion*

[55] Information Security Forum (ISF). *The ISF Standard of Good Practice for Information Security2020*. Available at https://www.securityforum.org/solutions-and-insights/standard-of-good-practice-for-information-security/

[56] ITIL® Foundation, ITIL 4 edition, AXELOS, February 2019, ISBN: 9780113316076

[57] National Institute of Standards and Technology (NIST), SP 800-37, *Risk Management Framework for Information Systems and Organizations: A System Lifecycle Approach for Security and Privacy, Revision 2. December2018* [viewed 2023-08-09]. Available at https://doi.org/10.6028/NIST.SP.800-37r2

[58] Open Web Application Security Project (OWASP). *OWASP Top Ten - 2021, The Ten Most Critical Web Application Security Risks*, 2021 [viewed 2023-08-09]. Available at https://owasp.org/Top10/

[59] Open Web Application Security Project (OWASP). *OWASP Developer Guide*, [online] [viewed 2023-08-09]. Available at https://owasp.org/www-project-developer-guide/

[60] Open Web Application Security Project (OWASP). *OWASP Top 10 API Security Risks – 2023*, [online] [viewed 2023-08-09]. Available at https://owasp.org/API-Security/editions/2023/en/0x11-t10/

[61] National Institute of Standards and Technology (NIST), SP 800-63B, *Digital Identity Guidelines; Authentication and Lifecycle Management*. February 2020 [viewed 2023-08-09]. Available at https://doi.org/10.6028/NIST.SP.800-63b

[62] OASIS, *Structured Threat Information Expression*. Available at https://www.oasis-open.org/standards#stix2.0

[63] OASIS, *Trusted Automated Exchange of Indicator Information*. Available at https://www.oasis-open.org/standards#taxii2.0

[64] ISO 31700-1:2023, *Consumer protection — Privacy by design for consumer goods and services — Part 1: High-level requirements*

[65] ISO/TR 31700-2:2023, *Consumer protection — Privacy by design for consumer goods and services — Part 2: Use cases*

ICS 35.030
Price based on 35 pages

iso.org