



DPC: 24/30482288 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 02 May 2024

Origin: International

Latest date for receipt of comments: 23 June 2024

Project No. 2023/02591

Responsible committee: IST/33/5 Identity Management and Privacy Technologies

Interested committees:

Title: Draft BS EN ISO/IEC 27018 Draft ISO/IEC 27018 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.

Please notify admin.start@bsigroup.com if you are aware of any keywords that might assist in clarifying or identifying the standard or of the content of this standard:

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 23 June 2024

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

E-mail: admin.start@bsigroup.com

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



DRAFT International Standard

ISO/IEC DIS 27018

Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII

ICS: 35.030

ISO/IEC JTC 1/SC 27

Secretariat: **DIN**

Voting begins on:
2024-04-30

Voting terminates on:
2024-07-23

This document is circulated as received from the committee secretariat.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

Reference number
ISO/IEC DIS 27018:2024(en)

Full document details: 24/30482288 DC

 **Documents**
Document Sharing Hub
© ISO/IEC 2024



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

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

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

Published in Switzerland

© ISO/IEC 2024 – All rights reserved

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Overview	3
4.1 Structure of this document	3
4.2 Control layout	7
5 Organizational controls	8
5.1 Policies for information security	8
5.2 Information security roles and responsibilities	8
5.3 Segregation of duties	9
5.4 Management responsibilities	9
5.5 Contact with authorities	9
5.6 Contact with special interest groups	9
5.7 Threat intelligence *	9
5.8 Information security in project management	9
5.9 Inventory of information and other associated assets	9
5.10 Acceptable use of information and other associated assets	9
5.11 Return of assets	9
5.12 Classification of information	9
5.13 Labelling of information	9
5.14 Information transfer	10
5.15 Access control	10
5.16 Identity management	10
5.17 Authentication information	10
5.18 Access rights	10
5.19 Information security in supplier relationships	10
5.20 Addressing information security within supplier agreements	10
5.21 Managing information security in the ICT supply chain	10
5.22 Monitoring, review and change management of supplier services	11
5.23 Information security for use of cloud services *	11
5.24 Information security incident management planning and preparation	11
5.25 Assessment and decision on information security events	11
5.26 Response to information security incidents	11
5.27 Learning from information security incidents	11
5.28 Collection of evidence	11
5.29 Information security during disruption	11
5.30 ICT readiness for business continuity *	11
5.31 Legal, statutory, regulatory and contractual requirements	11
5.32 Intellectual property rights	12
5.33 Protection of records	12
5.34 Privacy and protection of PII	12
5.35 Independent review of information security	12
5.36 Compliance with policies, rules and standards for information security	12
5.37 Documented operating procedures	12
6 People controls	12
6.1 Screening	12
6.2 Terms and conditions of employment	12
6.3 Information security awareness, education and training	12
6.4 Disciplinary process	13
6.5 Responsibilities after termination or change of employment	13
6.6 Confidentiality or non-disclosure agreements	13

6.7	Remote working	13
6.8	Information security event reporting	13
7	Physical controls	13
7.1	Physical security perimeters	13
7.2	Physical entry	13
7.3	Securing offices, rooms and facilities	13
7.4	Physical security monitoring *	13
7.5	Protecting against physical and environmental threats	13
7.6	Working in secure areas	13
7.7	Clear desk and clear screen	14
7.8	Equipment siting and protection	14
7.9	Security of assets off-premises	14
7.10	Storage media	14
7.11	Supporting utilities	14
7.12	Cabling security	14
7.13	Equipment maintenance	14
7.14	Secure disposal or re-use of equipment	14
8	Technological controls	14
8.1	User endpoint devices	14
8.2	Privileged access rights	14
8.3	Information access restriction	14
8.4	Access to source code	15
8.5	Secure authentication	15
8.6	Capacity management	15
8.7	Protection against malware	15
8.8	Management of technical vulnerabilities	15
8.9	Configuration management *	15
8.10	Information deletion *	15
8.11	Data masking *	15
8.12	Data leakage prevention *	15
8.13	Information backup	15
8.14	Redundancy of information processing facilities	16
8.15	Logging	16
8.16	Monitoring activities *	16
8.17	Clock synchronization	17
8.18	Use of privileged utility programs	17
8.19	Installation of software on operational systems	17
8.20	Networks security	17
8.21	Security of network services	17
8.22	Segregation of networks	17
8.23	Web filtering *	17
8.24	Use of cryptography	17
8.25	Secure development life cycle	17
8.26	Application security requirements	17
8.27	Secure system architecture and engineering principles	17
8.28	Secure coding *	17
8.29	Security testing in development and acceptance	18
8.30	Outsourced development	18
8.31	Separation of development, test and production environments	18
8.32	Change management	18
8.33	Test information	18
8.34	Protection of information systems during audit testing	18
	Annex A (normative) Public cloud PII processor extended control set for PII protection	19
	Annex B (informative) Correspondence of ISO/IEC 27018:202X (this document) with ISO/IEC 27018:2019	27
	Bibliography	30

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

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

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

OR (~initial editor's proposal, with modifications)

This edition cancels and replaces the second edition (ISO/IEC 27018: 2019), of which it constitutes a minor revision.

OR (Italian proposal, with modifications)

This 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 the most recent editions of ISO/IEC 27002;
- Annex XX 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.

Introduction

0.1 Background and context

Cloud service providers who process Personally Identifiable Information (PII) under contract to their customers need 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 multinational.

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, a “PII principal”, processing his or her own PII in the cloud, to an organization, 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 it under its contract with the public cloud PII processor. Note that 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 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. It has the following objectives:

- to help the public cloud service provider to comply with applicable obligations when acting as a PII processor, whether such obligations fall on the PII processor directly or through contract;
- 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 individual cloud service customer audits of data hosted in a multi-party, virtualized server (cloud) environment can be impractical technically and can increase risks to those physical and logical network security controls in place.

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.

Typically, an organization implementing ISO/IEC 27001 is protecting its own information assets. However, 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 augments 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 augments ISO/IEC 27002 in two ways:

- implementation guidance applicable to public cloud PII protection is provided for certain of the existing ISO/IEC 27002 controls, and
- [Annex A](#) provides a set of additional controls and associated guidance intended to address public cloud PII protection requirements not addressed by the existing ISO/IEC 27002 control set.

Most of the controls and guidance 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.

- Legal, Statutory, Regulatory and Contractual Requirements:** One source is the legal, statutory, regulatory and contractual requirements and obligations that an organization, its trading partners, contractors and service providers have to satisfy, and their socio-cultural responsibilities 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.
- 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, threats are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated. 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 guidance on privacy impact assessment.
- Corporate policies:** While many aspects covered by a corporate policy are derived from legal and socio-cultural obligations, 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 scope). 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 “sector-specific” is used in this document, as this is the conventional term used within other standards in the ISO/IEC 27000 series.

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 and regulations. Where controls from this document are not selected, this needs to be documented with justification for the omission.

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 17789). 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 need to clearly 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 below 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 Bibliographic entry [9]).

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 storage, processing, use and transmission to its eventual destruction or decay. The risks to PII can vary during its lifetime but protection of PII remains important to some extent at all stages.

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

Information technology — Security techniques — Code of practice 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 29100:2011 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. However, PII controllers can be subject to additional PII protection legislation, regulations and obligations, not applying to PII processors. This document is not intended to cover such additional obligations.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 17788, *Information technology — Cloud computing — Overview and vocabulary*

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

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27002:2022 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 27040:2015, 3.7]

3.2**personally identifiable information****PII**

any 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 29100:2011/Amd 1:2018, 2.9, 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 29100:2011, 2.10]

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 29100:2011, 2.11]

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 29100:2011, 2.12]

3.6**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 29100:2011, 2.23]

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 (which superseded ISO/IEC 27002:2013) 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 has been repeated here.

The structure used for expressing controls (control layout) in ISO/IEC 27002:2022 is considerably different from the one used in ISO/IEC 27002:2013. The most significant change is that the controls categorized under a two layered structure consisting of the top layer with 14 control clauses and the second layer with 35 control categories in the older version are now categorized under a single layer consisting of 5 themes. Also, the total number of controls in the older version was 114 while in the new version it is 93, as a consequence of merging two or more controls into a single control in some instances and adding some new controls as well. The comparison of the two control layouts is given in a table in [Appendix B](#).

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 [clause 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 & 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 “Sector-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.

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

Legend:

- *Sector-specific implementation guidance is provided: Public cloud PII protection implementation guidance*
- *Sector-specific implementation guidance and other information is provided: Public cloud PII protection implementation guidance and other information for Public cloud PII protection*
- *No additional sector-specific implementation guidance or other information is provided: no specific Guidance or other information for Public cloud PII protection*
- *Sector-specific implementation guidance is provided, together with a cross-reference to control(s) in [Annex A](#): Public cloud PII protection implementation guidance and cross-reference to control(s) in [Annex A](#)*

NOTE The 11 controls that are new in ISO/IEC 27002:2022 are marked with * in Table 1 as well as in the chapters 5-8.

ISO/IEC 27002:2022 Control identifier	ISO/IEC 27002:2022 Control name	Remarks
Clause 5 - Organizational controls		
5.1	Policies for information security	Sector-specific implementation guidance and other information is provided.
5.2	Information security roles and responsibilities	Sector-specific implementation guidance is provided.
5.3	Segregation of duties	No additional sector-specific implementation guidance or other information is provided.
5.4	Management responsibilities	No additional sector-specific implementation guidance or other information is provided.