



DPC: 24/30496044 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 July 2024

Origin: International

Latest date for receipt of comments: 28 July 2024

Project No. 2022/02452

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

Interested committees:

Title: Draft BS EN ISO/IEC 27701 BS EN ISO/IEC 27701 Information security, cybersecurity and privacy protection -Privacy information management systems - Requirements and guidance.

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 28 July 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/>.

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 27701.2

Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance

ICS: 35.030

ISO/IEC JTC 1/SC 27

Secretariat: **DIN**

Voting begins on:
2024-07-02

Voting terminates on:
2024-08-27

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

IMPORTANT — Please use this updated version dated 2024-06-19, and discard any previous version of this DIS as VA relation has been added.

Reference number
ISO/IEC DIS 27701.2:2024(en)

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.

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



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

Contents

Page

Foreword.....	viii
Introduction.....	ix
1 Scope	1
2 Normative references	1
3 Terms, definitions and abbreviations.....	1
4 Context of the organization.....	5
4.1 Understanding the organization and its context.....	5
4.2 Understanding the needs and expectations of interested parties.....	5
4.3 Determining the scope of the privacy information management system.....	6
4.4 Privacy information management system.....	6
5 Leadership.....	7
5.1 Leadership and commitment.....	7
5.2 Privacy Policy.....	7
5.3 Roles, responsibilities and authorities.....	7
6 Planning.....	8
6.1 Actions to address risks and opportunities.....	8
6.1.1 General.....	8
6.1.2 Privacy risk assessment.....	8
6.1.3 Privacy risk treatment.....	9
6.2 Privacy objectives and planning to achieve them.....	10
6.3 Planning of changes.....	10
7 Support.....	10
7.1 Resources.....	10
7.2 Competence.....	10
7.3 Awareness.....	11
7.4 Communication.....	11
7.5 Documented information.....	11
7.5.1 General.....	11
7.5.2 Creating and updating documented information.....	11
7.5.3 Control of documented information.....	12
8 Operation.....	12
8.1 Operational planning and control.....	12
8.2 Privacy risk assessment.....	12
8.3 Privacy risk treatment.....	13
9 Performance evaluation.....	13
9.1 Monitoring, measurement, analysis and evaluation.....	13
9.2 Internal audit.....	13
9.2.1 General.....	13
9.2.2 Internal audit programme.....	13
9.3 Management review.....	14
9.3.1 General.....	14
9.3.2 Management review inputs.....	14

9.3.3	Management review results	14
10	Improvement	14
10.1	Continual improvement.....	14
10.2	Nonconformity and corrective action.....	14
11	Further information on Annexes.....	15
Annex A	(normative) PIMS reference control objectives and controls for PII Controllers and PII Processors.....	16
Annex B	(normative) Implementation guidance for PII Controllers and PII processors.....	23
B.1	Implementation guidance for PII controllers	23
B.1.1	General.....	23
B.1.2	Conditions for collection and processing.....	23
B.1.2.1	Objective.....	23
B.1.2.2	Identify and document purpose.....	23
B.1.2.3	Identify lawful basis	23
B.1.2.4	Determine when and how consent is to be obtained	24
B.1.2.5	Obtain and record consent	24
B.1.2.6	Privacy impact assessment.....	25
B.1.2.7	Contracts with PII processors.....	25
B.1.2.8	Joint PII controller	26
B.1.2.9	Records related to processing PII	26
B.1.3	Obligations to PII principals.....	27
B.1.3.1	Objective.....	27
B.1.3.2	Determining and fulfilling obligations to PII principals	27
B.1.3.3	Determining information for PII principals.....	27
B.1.3.4	Providing information to PII principals.....	28
B.1.3.5	Providing mechanism to modify or withdraw consent	28
B.1.3.6	Providing mechanism to object to PII processing	29
B.1.3.7	Access, correction or erasure	29
B.1.3.8	PII controllers' obligations to inform third parties.....	30
B.1.3.9	Providing copy of PII processed.....	30
B.1.3.10	Handling requests	30
B.1.3.11	Automated decision making.....	31
B.1.4	Privacy by design and privacy by default.....	31
B.1.4.1	Objective.....	31
B.1.4.2	Limit collection	31
B.1.4.3	Limit processing	31
B.1.4.4	Accuracy and quality.....	32

B.1.4.5 PII minimization objectives	32
B.1.4.6 PII de-identification and deletion at the end of processing	33
B.1.4.7 Temporary files	33
B.1.4.8 Retention	33
B.1.4.9 Disposal	34
B.1.4.10 PII transmission controls	34
B.1.5 PII sharing, transfer and disclosure	34
B.1.5.1 Objective	34
B.1.5.2 Identify basis for PII transfer between jurisdictions	34
B.1.5.3 Countries and international organizations to which PII can be transferred	35
B.1.5.4 Records of transfer of PII	35
B.1.5.5 Records of PII disclosure to third parties	35
B.2 Implementation guidance for PII processors	35
B.2.1 General	35
B.2.2 Conditions for collection and processing	36
B.2.2.1 Objective	36
B.2.2.2 Customer agreement	36
B.2.2.3 Organization's purposes	36
B.2.2.4 Marketing and advertising use	37
B.2.2.5 Infringing instruction	37
B.2.2.6 Customer obligations	37
B.2.2.7 Records related to processing PII	37
B.2.3 Obligations to PII principals	37
B.2.3.1 Objective	38
B.2.3.2 Comply with obligations to PII principals	38
B.2.4 Privacy by design and privacy by default	38
B.2.4.1 Objective	38
B.2.4.2 Temporary files	38
B.2.4.3 Return, transfer or disposal of PII	38
B.2.4.4 PII transmission controls	39
B.2.5 PII sharing, transfer and disclosure	39
B.2.5.1 Objective	39
B.2.5.2 Basis for PII transfer between jurisdictions	39
B.2.5.3 Countries and international organizations to which PII can be transferred	40
B.2.5.4 Records of PII disclosures to third parties	40
B.2.5.5 Notification of PII disclosure requests	40

B.2.5.6 Legally binding PII disclosures	41
B.2.5.7 Disclosure of subcontractors used to process PII	41
B.2.5.8 Engagement of a subcontractor to process PII	41
B.2.5.9 Change of subcontractor to process PII.....	42
B.3 Implementation guidance for PII controllers and PII processors	42
B.3.1 Objective.....	42
B.3.2 General	42
B.3.3 Policies for information security.....	42
B.3.4 Information security roles and responsibilities	42
B.3.5 Classification of information.....	43
B.3.6 Labelling of information	43
B.3.7 Information transfer	43
B.3.8 Identity management	44
B.3.9 Access rights.....	44
B.3.10 Addressing information security within supplier agreements	44
B.3.11 Information security incident management planning and preparation.....	45
B.3.12 Response to information security incidents	45
B.3.13 Legal, statutory, regulatory and contractual requirements	47
B.3.14 Protection of records	47
B.3.15 Independent review of information security	47
B.3.16 Compliance with policies, rules and standards for information security	48
B.3.17 Information security awareness, education and training.....	48
B.3.18 Confidentiality or non-disclosure agreements.....	48
B.3.19 Clear desk and clear screen.....	49
B.3.20 Storage media.....	49
B.3.21 Secure disposal or re-use of equipment	49
B.3.22 User endpoint devices	50
B.3.23 Secure authentication.....	50
B.3.24 Information backup	50
B.3.25 Logging.....	51
B.3.26 Use of cryptography	51
B.3.27 Secure development life cycle	52
B.3.28 Application security requirements.....	52
B.3.29 Secure system architecture and engineering principles	52
B.3.30 Outsourced development.....	53
B.3.31 Test information.....	53

Annex C (informative) Mapping to ISO/IEC 29100	54
Annex D (informative) Mapping to the General Data Protection Regulation	57
Annex E (informative) Mapping to ISO/IEC 27018 and ISO/IEC 29151	61
Annex F (informative) Correspondence with ISO/IEC 27701:2019	64
Bibliography	72

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 second edition cancels and replaces the first edition (ISO/IEC 27701:2019), which has been redrafted as a stand-alone management system.

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 General

Almost every organization processes personally identifiable information (PII). Further, the quantity and types of PII processed is increasing, as is the number of situations where an organization needs to cooperate with other organizations regarding the processing of PII. Protection of privacy in the context of the processing of PII is a societal need, as well as the topic of dedicated legislation or regulation all over the world.

This document includes mapping to:

- the privacy framework and principles defined in ISO/IEC 29100;
- ISO/IEC 27018;
- ISO/IEC 29151; and
- the EU General Data Protection Regulation.

NOTE These can be interpreted to take into account local legislation or regulation.

This document can be used by PII controllers (including those that are joint PII controllers) and PII processors (including those using subcontracted PII processors and those processing PII as subcontractors to PII processors).

By complying with the requirements in this document, an organization can generate evidence of how it handles the processing of PII. Such evidence can be used to facilitate agreements with business partners where the processing of PII is mutually relevant. This can also assist in relationships with other interested parties. The use of this document can provide independent verification of this evidence.

This document was initially developed as ISO/IEC 27552.

0.2 Compatibility with other management system standards

This document applies the framework developed by ISO to improve alignment among its management system standards.

This document enables an organization to align or integrate its PIMS with the requirements of other management system standards, and in particular with the information security management system specified in ISO/IEC 27001.

Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance

1 Scope

This document specifies requirements for establishing, implementing, maintaining and continually improving a privacy information management system (PIMS).

Guidance is provided to assist in the implementation of the requirements in this document.

This document is intended for PII controllers and PII processors holding responsibility and accountability for PII processing.

This document is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations.

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 29100, *Information technology — Security techniques — Privacy framework*

3 Terms, definitions and abbreviations

For the purposes of this document, the terms and definitions given in ISO/IEC 29100 and the following apply.

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

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

3.1

organization

person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its *objectives* (3.6)

Note 1 to entry: The concept of organization includes, but is not limited to, sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

Note 2 to entry: If the organization is part of a larger entity, the term “organization” refers only to the part of the larger entity that is within the scope of the privacy information *management system* (3.4).

3.2

interested party (preferred term)

stakeholder (admitted term)

person or *organization* (3.1) that can affect, be affected by, or perceive itself to be affected by a decision or activity

3.3

top management

person or group of people who directs and controls an *organization* (3.1) at the highest level

Note 1 to entry: Top management has the power to delegate authority and provide resources within the organization.

Note 2 to entry: If the scope of the *management system* (3.4) covers only part of an organization, then top management refers to those who direct and control that part of the organization.

3.4

management system

set of interrelated or interacting elements of an *organization* (3.1) to establish *policies* (3.5) and *objectives* (3.6), as well as *processes* (3.8) to achieve those objectives

Note 1 to entry: A management system can address a single discipline or several disciplines.

Note 2 to entry: The management system elements include the organization's structure, roles and responsibilities, planning and operation.

3.5

policy

intentions and direction of an *organization* (3.1) as formally expressed by its *top management* (3.3)

3.6

objective

result to be achieved

Note 1 to entry: An objective can be strategic, tactical, or operational.

Note 2 to entry: Objectives can relate to different disciplines (such as finance, health and safety, and environment). They can be, for example, organization-wide or specific to a project, product or *process* (3.8).

Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended result, as a purpose, as an operational criterion, as a privacy information objective or by the use of other words with similar meaning (e.g. aim, goal, or target).

Note 4 to entry: In the context of *privacy information management systems* (3.22), privacy information objectives are set by the *organization* (3.1), consistent with the privacy information *policy* (3.5), to achieve specific results.

3.7

risk

effect of uncertainty

Note 1 to entry: An effect is a deviation from the expected — positive or negative.

Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

Note 3 to entry: Risk is often characterized by reference to potential events (as defined in ISO Guide 73) and consequences (as defined in ISO Guide 73), or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood (as defined in ISO Guide 73) of occurrence.

3.8

process

set of interrelated or interacting activities that uses or transforms inputs to deliver a result

Note 1 to entry: Whether the result of a process is called an output, a product or a service depends on the context of the reference.

3.9

competence

ability to apply knowledge and skills to achieve intended results

3.10

documented information

information required to be controlled and maintained by an *organization* (3.1) and the medium on which it is contained

Note 1 to entry: Documented information can be in any format and media and from any source.

Note 2 to entry: Documented information can refer to: – the *management system* (3.4), including related *processes* (3.8); – information created in order for the organization to operate (documentation); – evidence of results achieved (records).

3.11

performance

measurable result

Note 1 to entry: Performance can relate either to quantitative or qualitative findings.

Note 2 to entry: Performance can relate to managing activities, *processes* (3.8), products, services, systems or *organizations* (3.1).

3.12

continual improvement

recurring activity to enhance *performance* (3.11)

3.13

effectiveness

extent to which planned activities are realized and planned results are achieved

3.14

requirement

need or expectation that is stated, generally implied or obligatory

Note 1 to entry: “Generally implied” means that it is custom or common practice for the *organization* (3.1) and *interested parties* (3.2) that the need or expectation under consideration is implied.

Note 2 to entry: A specified requirement is one that is stated, e.g. in *documented information* (3.10).

3.15

conformity

fulfilment of a *requirement* (3.14)

3.16

nonconformity

non-fulfilment of a *requirement* (3.14)

3.17

corrective action

action to eliminate the cause(s) of a *nonconformity* (3.16) and to prevent recurrence

3.18

audit

systematic and independent *process* (3.8) for obtaining evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

Note 1 to entry: An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines).

Note 2 to entry: An internal audit is conducted by the *organization* (3.1) itself, or by an external party on its behalf.

Note 3 to entry: "Audit evidence" and "audit criteria" are defined in ISO 19011.

3.19

measurement

process (3.8) to determine a value

3.20

monitoring

determining the status of a system, a *process* (3.8) or an activity

Note 1 to entry: To determine the status, there can be a need to check, supervise or critically observe.

3.21

joint PII controller

PII controller that determines the purposes and means of the processing of PII jointly with one or more other PII controllers

3.22

customer

person or *organization* (3.1) that could or does receive a product or a service that is intended for or required by this person or *organization* (3.1)

EXAMPLE Consumer, client, end-user, retailer, receiver of product or service from an internal *process* (3.8), beneficiary and purchaser.

Note 1 to entry: A customer can be internal or external to the organization.

Note 2 to entry: A customer can be an *organization* (3.1) that has a contract with a PII controller, a PII controller who has a contract with a PII processor or a PII processor that has a contract with a subcontractor for PII processing (see 4.2 for further information).

3.23

privacy information management system

PIMS

management system (3.4) which addresses the protection of privacy as potentially affected by the processing of PII

3.24

information security programme

set of policies (3.5), objectives (3.6) and processes (3.8) designed to manage risks (3.7) to an organization's (3.1) assets, to ensure confidentiality, integrity and availability of information

Note 1 to entry: An information security programme can be, for example, an information security management system such as one based on ISO/IEC 27001.

3.25

statement of applicability

documentation of all necessary controls and justification for inclusion or exclusion of controls

Note 1 to entry: Organizations may not require all controls listed in Annex A or may even exceed the list in Annex A with additional controls established by the organization itself.

4 Context of the organization

4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended result(s) of its privacy information management system.

The organization shall determine whether climate change is a relevant issue.

The organization shall determine if it is acting as a PII controller (including as a joint PII controller) or as a PII processor.

The organization shall determine external and internal issues that are relevant to its context and that affect its ability to achieve the intended outcome(s) of its PIMS.

NOTE 1 External and internal issues can include but are not limited to:

- applicable privacy legislation;
- applicable regulations;
- applicable judicial decisions;
- applicable organizational context, governance, policies and procedures;
- applicable administrative decisions;
- applicable contractual requirements.

Where the organization acts in both roles (i.e. a PII controller and a PII processor), separate roles shall be determined, each of which is the subject of a separate set of controls.

NOTE 2 The role of the organization can be different for each instance of the processing of PII, since it depends on who determines the purposes and means of the processing.

4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

- the interested parties that are relevant to the privacy information management system;
- the relevant requirements of these interested parties;
- which of these requirements will be addressed through the privacy information management system.

NOTE 1 Relevant interested parties can have requirements related to climate change.

The organization shall include among its interested parties those parties having interests or responsibilities associated with the processing of PII, including the PII principals.

NOTE 2 Other interested parties can include customers (see 4.2), supervisory authorities, other PII controllers, PII processors and their subcontractors.

Depending on the role of the organization, "customer" can be understood as either:

- a) an organization who has a contract with a PII controller (e.g. the customer of the PII controller, the case of an organization which is a joint PII controller);
- b) a PII controller who has a contract with a PII processor (e.g. the customer of the PII processor); or
- c) a PII processor who has a contract with a subcontractor for PII processing (e.g. the customer of the subcontracted PII processor).

NOTE 3 An individual person in a business to consumer relationship with an organization is referred to as a "PII principal" in this document.

NOTE 4 Requirements relevant to the processing of PII can be determined by legal and regulatory requirements, by contractual obligations and by self-imposed organizational objectives. The privacy principles set out in ISO/IEC 29100 provide guidance concerning the processing of PII.

NOTE 5 As an element to demonstrate compliance to the organization's obligations, some interested parties can expect that the organization is in conformity with specific standards, such as the management system specified in this document, or any relevant set of specifications. These parties can call for independently audited compliance to these standards.

4.3 Determining the scope of the privacy information management system

The organization shall determine the boundaries and applicability of the privacy information management system to establish its scope.

When determining this scope, the organization shall consider:

- the external and internal issues referred to in 4.1;
- the requirements referred to in 4.2.

The scope of the organization's privacy information system shall be available and be maintained as documented information.

When determining the scope of the PIMS, the organization shall include the processing of PII.

4.4 Privacy information management system

The organization shall establish, implement, maintain and continually improve a privacy information management system, including the processes needed and their interactions, in accordance with the requirements of this document.

5 Leadership

5.1 Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the privacy information management system by:

- ensuring that the privacy policy (see 5.2) and privacy objectives (see 6.2) are established and are compatible with the strategic direction of the organization;
- ensuring the integration of the privacy information management system requirements into the organization's business processes;
- ensuring that the resources needed for the privacy information management system are available;
- communicating the importance of effective privacy information management and of conforming to the privacy information management system requirements;
- ensuring that the privacy information management system achieves its intended result(s);
- directing and supporting persons to contribute to the effectiveness of the privacy information management system;
- promoting continual improvement;
- supporting other relevant roles to demonstrate their leadership as it applies to their areas of responsibility.

NOTE Reference to "business" in this document can be interpreted broadly to mean those activities that are core to the purposes of the organization's existence.

5.2 Privacy Policy

Top management shall establish a privacy policy that:

- a) is appropriate to the purpose of the organization;
- b) provides a framework for setting privacy objectives;
- c) includes a commitment to meet applicable requirements;
- d) includes a commitment to continual improvement of the privacy information management system.

The privacy policy shall:

- be available as documented information;
- be communicated within the organization;
- be available to interested parties, as appropriate.

5.3 Roles, responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the organization.

Top management shall assign the responsibility and authority for:

- a) ensuring that the privacy information management system conforms to the requirements of this document;
- b) reporting on the performance of the privacy information management system to top management.

6 Planning

6.1 Actions to address risks and opportunities

6.1.1 General

When planning for the privacy information management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:

- give assurance that the privacy information management system can achieve its intended result(s);
- prevent, or reduce undesired effects;
- achieve continual improvement.

The organization shall plan:

- a) actions to address these risks and opportunities;
 - b) how to
- integrate and implement the actions into its privacy information management system processes;
 - evaluate the effectiveness of these actions.

6.1.2 Privacy risk assessment

The organization shall define and apply a privacy risk assessment process that:

- a) establishes and maintains privacy risk criteria that include:
 - 1) the risk acceptance criteria; and
 - 2) criteria for performing privacy risk assessments;
- b) ensures that repeated privacy risk assessments produce consistent, valid and comparable results;
- c) identifies the privacy risks:
 - 1) associated with the protection of privacy and information security risks within the scope of the privacy information management system; and
 - 2) that identify the risk owners;
- d) analyses the privacy risks that:
 - 1) assess the potential consequences for both the organization and PII principals that would result if the risks identified in [6.1.2 c\) 1\)](#) were to materialize;

- 2) assess the realistic likelihood of the occurrence of the risks identified in [6.1.2 c\) 1\)](#); and
 - 3) determine the levels of risk;
- e) evaluates the privacy risks that:
- 1) compare the results of risk analysis with the risk criteria established in [6.1.2 a\)](#); and
 - 2) prioritize the analysed risks for risk treatment.

The organization shall retain documented information about the privacy risk assessment process.

NOTE For further information on the privacy risk assessment process, see ISO/IEC 27557.

6.1.3 Privacy risk treatment

The organization shall define and apply a privacy risk treatment process to treat risks related to the processing of PII, including risks to PII principals, and including the security of PII, by:

- a) selecting appropriate privacy risk treatment options, taking account of the risk assessment results;
- b) determining all controls that are necessary to implement the privacy risk treatment option(s) chosen;

NOTE 1 Organizations can design controls as required, or identify them from any source.

- c) identifying and documenting the information security programme implemented by the organization, including the appropriate security controls;

NOTE 2 ISO/IEC 27002 provides a list of possible information security controls. If the information security programme is based on ISO/IEC 27001, users of this document are directed to ISO/IEC 27002 to ensure that no necessary information security controls are overlooked.

- d) comparing the controls determined in [6.1.3 b\)](#) above with those in Annex A and verifying that no necessary controls have been omitted;

NOTE 3 Annex A contains a list of possible privacy controls. Users of this document are directed to Annex A to ensure that no necessary privacy controls are overlooked.

NOTE 4 The privacy controls listed in Annex A are not exhaustive and additional privacy controls can be included if needed.

NOTE 5 Organizations can address security and privacy in an integrated manner when considering the security of PII processing, combining security and privacy risk assessments for example, or as separate entities with overlapping areas.

- e) producing a statement of applicability that includes;
 - the necessary controls (see [6.1.3 b\)](#), [c\)](#) and [d\)](#));
 - justification for their inclusion;
 - whether the necessary controls are implemented or not; and
 - the justification for excluding any of the controls from Annex A.

Not all the controls listed in Annex A need to be included. Justification for exclusion of any control can include where the controls are not deemed necessary by the risk assessment, and where they are not required by (or are subject to exceptions under) the applicable legislation or regulation, including those applicable to the PII principal.

- f) formulating a privacy risk treatment plan;
- g) obtaining the privacy risk owners' approval of the privacy risk treatment plan and acceptance of the residual privacy risks; and
- h) considering the guidance in Annex B for the implementation of controls determined in b) and c).

The organization shall retain documented information about the information privacy risk treatment process.

6.2 Privacy objectives and planning to achieve them

The organization shall establish privacy objectives at relevant functions and levels.

The privacy objectives shall:

- a) be consistent with the privacy policy (see 5.2);
- b) be measurable (if practicable);
- c) take into account applicable requirements;
- d) be monitored;
- e) be communicated;
- f) be updated as appropriate;
- g) be available as documented information.

When planning how to achieve its privacy objectives, the organization shall determine:

- what will be done;
- what resources will be required;
- who will be responsible;
- when it will be completed;
- how the results will be evaluated.

6.3 Planning of changes

When the organization determines the need for changes to the privacy information management system, the changes shall be carried out in a planned manner.

7 Support

7.1 Resources

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the privacy information management system.

7.2 Competence

The organization shall:

- determine the necessary competence of person(s) doing work under its control that affects its **privacy information performance**;
- ensure that these persons are competent on the basis of appropriate education, training, or experience;
- where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken.

Appropriate documented information shall be available as evidence of competence.

NOTE Applicable actions can include, for example: the provision of training to, the mentoring of, or the re-assignment of currently employed persons; or the hiring or contracting of competent persons.

7.3 Awareness

Persons doing work under the organization's control shall be aware of:

- the **privacy policy** (see 5.2);
- their contribution to the effectiveness of the **privacy information management system**, including the benefits of improved **privacy performance**;
- the implications of not conforming with the **privacy information management system** requirements.

7.4 Communication

The organization shall determine the internal and external communications relevant to the **privacy information management system** including:

- on what it will communicate;
- when to communicate;
- with whom to communicate;
- how to communicate.

7.5 Documented information

7.5.1 General

The organization's **privacy information management system** shall include:

- a) documented information required by this document;
- b) documented information determined by the organization as being necessary for the effectiveness of the **privacy information management system**.

NOTE The extent of documented information for a **privacy information management system** can differ from one organization to another due to:

- the size of organization and its type of activities, processes, products and services;
- the complexity of processes and their interactions;
- the competence of persons.

7.5.2 Creating and updating documented information

When creating and updating documented information, the organization shall ensure appropriate:

- identification and description (e.g. a title, date, author, or reference number);

- format (e.g. language, software version, graphics) and media (e.g. paper, electronic);
- review and approval for suitability and adequacy.

7.5.3 Control of documented information

Documented information required by the privacy information management system and by this document shall be controlled to ensure:

- a) it is available and suitable for use, where and when it is needed;
- b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

For the control of documented information, the organization shall address the following activities, as applicable:

- distribution, access, retrieval and use;
- storage and preservation, including preservation of legibility;
- control of changes (e.g. version control);
- retention and disposition.

Documented information of external origin determined by the organization to be necessary for the planning and operation of the privacy information management system shall be identified as appropriate and controlled.

NOTE Access can imply a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information.

8 Operation

8.1 Operational planning and control

The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Clause 6, by:

- establishing criteria for the processes;
- implementing control of the processes in accordance with the criteria.

Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned.

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that externally provided processes, products or services that are relevant to the privacy information management system are controlled.

8.2 Privacy risk assessment

The organization shall perform privacy risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a).

The organization shall retain documented information of the results of the privacy risk assessments.

8.3 Privacy risk treatment

The organization shall implement the privacy risk treatment plan.

The organization shall retain documented information of the results of the privacy risk treatment.

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

The organization shall determine:

- what needs to be monitored and measured;
- the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;
- when the monitoring and measuring shall be performed;
- when the results from monitoring and measurement shall be analysed and evaluated.

Documented information shall be available as evidence of the results.

The organization shall evaluate the privacy performance and the effectiveness of the privacy information management system.

9.2 Internal audit

9.2.1 General

The organization shall conduct internal audits at planned intervals to provide information on whether the privacy information management system:

- a) conforms to:
 - the organization's own requirements for its privacy information management system;
 - the requirements of this document;
- b) is effectively implemented and maintained.

9.2.2 Internal audit programme

The organization shall plan, establish, implement and maintain (an) audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting.

When establishing the internal audit programme(s), the organization shall consider the importance of the processes concerned and the results of previous audits.

The organization shall:

- a) define the audit objectives, criteria and scope for each audit;
- b) select auditors and conduct audits to ensure objectivity and the impartiality of the audit process;
- c) ensure that the results of audits are reported to relevant managers.

Documented information shall be available as evidence of the implementation of the audit programme(s) and the audit results.

9.3 Management review

9.3.1 General

Top management shall review the organization's privacy information management system, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness.

9.3.2 Management review inputs

The management review shall include:

- a) the status of actions from previous management reviews;
- b) changes in external and internal issues that are relevant to the privacy information management system;
- c) changes in needs and expectations of interested parties that are relevant to the privacy information management system;
- d) information on the privacy information management system performance, including trends in:
 - nonconformities and corrective actions;
 - monitoring and measurement results;
 - audit results;
- d) opportunities for continual improvement.

9.3.3 Management review results

The results of the management review shall include decisions related to continual improvement opportunities and any need for changes to the privacy information management system.

Documented information shall be available as evidence of the results of management reviews.

10 Improvement

10.1 Continual improvement

The organization shall continually improve the suitability, adequacy and effectiveness of the privacy information management system.

10.2 Nonconformity and corrective action

When a nonconformity occurs, the organization shall:

- a) react to the nonconformity, and as applicable:
 - take action to control and correct it;
 - deal with the consequences;
- b) evaluate the need for action to eliminate the cause(s) of the nonconformity, in order that it does not recur or occur elsewhere, by:
 - reviewing the nonconformity;
 - determining the causes of the nonconformity;
 - determining if similar nonconformities exist, or can potentially occur;
- c) implement any action needed;
- d) review the effectiveness of any corrective action taken;
- e) make changes to the privacy information management system, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered.