INTERNATIONAL STANDARD

ISO/IEC 27557

First edition
2022-11

Information security, cybersecurity and privacy protection — Application of ISO 31000:2018 for organizational privacy risk management

Sécurité de l'information, cybersécurité et protection de la vie privée — Application de l'ISO 31000:2018 au management des risques organisationnels liés à la vie privée

Reference number
ISO/IEC 27557:2022(E)

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).

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) or the IEC list of patent declarations received (see https://patents.iec.ch).

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 JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

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

There is a growing interest in and need to address the differences between information security risk management and privacy risk management for organizations processing personally identifiable information (PII). Information security risk management and related risk assessments have traditionally focused on risk to an organization, often using the widely accepted formula of risk = impact x likelihood. Organizations can use various methods to assess and rank impacts and likelihood, and then determine a value (qualitative or quantitative) for organizational risk that can be used to prioritize risk mitigation.

Conversely, privacy assessments have primarily been focused on impacts on individuals, such as those identified through a privacy impact assessment. Although privacy assessments may prioritize the impacts on an individual's privacy, it is nonetheless necessary to consider how such privacy impacts on an individual can contribute to overall organizational risk. Doing so can help organizations build trust, implement technical and organisational measures, improve communication and support compliance with legal obligations, while avoiding negative impacts to reputation, bottom lines, and future prospects for growth. Privacy events may have consequences for the organization, even in the absence of adverse impacts on PII principals.

This document offers a framework for assessing organizational privacy risk, with consideration of the privacy impact on individuals as a component of overall organizational risk. It extends the guidelines of ISO 31000:2018 to include specific considerations for organizational privacy risk and supports the requirement for risk management as required by privacy information management systems (such as ISO/IEC 27701).

This document is intended to be used in connection with ISO 31000:2018. Whenever this document extends the guidance given in ISO 31000:2018, an appropriate reference to the clauses of ISO 31000:2018 is made followed by privacy-specific guidance. The clause structure of ISO 31000:2018 is mirrored in this document and amended by sub-clauses if needed.

Information security, cybersecurity and privacy protection — Application of ISO 31000:2018 for organizational privacy risk management

1 Scope

This document provides guidelines for organizational privacy risk management, extended from ISO 31000:2018.

This document provides guidance to organizations for integrating risks related to the processing of personally identifiable information (PII) as part of an organizational privacy risk management programme. It distinguishes between the impact that processing PII can have on an individual with consequences for organizations (e.g. reputational damage). It also provides guidance for incorporating the following into the overall organizational risk assessment:

— organizational consequences of adverse privacy impacts on individuals; and

— organizational consequences of privacy events that damage the organization (e.g. by harming its reputation) without causing any adverse privacy impacts to individuals.

This document assists in the implementation of a risk-based privacy program which can be integrated in the overall risk management of the organization.

This document is applicable to all types and sizes of organizations processing PII or developing products and services that can be used to process PII, including public and private companies, government entities, and non-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 31000:2018, *Risk management — Guidelines*

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

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 31000, ISO/IEC 29100 and ISO/IEC 27000 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
privacy information management system
PIMS
information security management system which addresses the protection of privacy as potentially affected by the processing of personally identifiable information (PII)

[SOURCE: ISO/IEC 27701:2019, 3.2 modified — the abbreviated term "PII" is expanded as "personally identifiable information".]

3.2
privacy event
occurrence or change of a particular set of circumstances related to personally identifiable information (PII) processing that can cause a *privacy impact* (3.3) or consequence

3.3
privacy impact
element that has an effect on the privacy of a personally identifiable information (PII) principal and/or group of PII principals

Note 1 to entry: The privacy impact could result from the processing of PII in conformance or in violation of privacy safeguarding requirements.

[SOURCE: ISO/IEC 29134:2017, 3.6, modified — "anything" replaced by "element".]

3.4
consequence
outcome of an event affecting organizational objectives

[SOURCE: ISO 31000:2018, 3.6, modified — "organizational" added and notes to entry removed]

4 Principles of organizational privacy risk management

The guidance in ISO 31000:2018, Clause 4 and the following additional guidance applies.

For organizational privacy risk management, PII principals should be included as stakeholders, and the actual or potential adverse impact on them should be included when considering risks. Additionally, the organization should consider the potential negative effect on the opinions and attitudes of these stakeholders related to the organization should these adverse impacts occur.

Organizations should identify the norms, societal values, and legal expectations related to individuals' privacy given their cultural context(s). Privacy is a broad and shifting concept that can be filtered through cultural diversity and individual differences. These cultural factors can inform the identification, evaluation, and treatment of privacy risks.

5 Framework

5.1 General

The guidance in ISO 31000:2018, 5.1 applies.

5.2 Leadership and commitment

The guidance in ISO 31000:2018, 5.2 and the following additional guidance applies.

Top management should be aware of privacy issues in order to successfully incorporate privacy considerations into an overall organizational risk management process. This should include awareness of such topics as:

— privacy regulations and laws applicable to the organization;

— privacy obligations the organization has to individuals;

— how processing PII can impact individuals;

— unique concerns, risks, vulnerabilities, impacts, and organizational consequences related to privacy and processing PII.

Where an organization implements a privacy information management system (PIMS) as specified in ISO/IEC 27701, the organization should be aware of and committed to integrating the organizational privacy risk management activities related to the relevant aspects of the PIMS.

5.3 Integration

The guidance in ISO 31000:2018, 5.3 and the following additional guidance applies.

Top management and oversight bodies should ensure that organizational privacy risk management is integrated into the organization's structure, including people, processes, and technology. The integration depends on the operating processes of the organization. Where an organization implements a PIMS, the organizational privacy risk management process should be integrated into the relevant aspects of the PIMS.

5.4 Design

5.4.1 Understanding the organization and its context

The guidance in ISO 31000:2018, 5.4.1 and the following additional guidance applies.

When an organization processes PII, or is developing products or services that process PII, the organization should assess its role related to processing PII (e.g. controller, processor, joint controller, manufacturer, software developer, provider of products that process PII).

Understanding the organization's role relative to processing PII is critical for the effective design of a risk management framework, including accurately identifying and treating privacy risks to the organization.

Where an organization implements a PIMS, this context should align with the context of the management system (ISO/IEC 27701:2019, 5.2.1).

5.4.2 Articulating risk management commitment

The guidance in ISO 31000:2018, 5.4.2 applies.

5.4.3 Assigning organizational roles, authorities, responsibilities and accountabilities

The guidance in ISO 31000:2018, 5.4.3 and the following additional guidance applies.

Top management and oversight bodies should:

— emphasize that risk management related to PII processing is a core responsibility;

— identify individuals who have the accountability and authority to manage risks related to PII processing;

— identify individuals who have the accountability and authority to manage risks related to privacy events that have direct consequences for the organization, even when there are no impacts on PII principals, employees or other stakeholders.

5.4.4 Allocating resources

The guidance in ISO 31000:2018, 5.4.4 and the following additional guidance applies.

When allocating resources for organizational privacy risk management, top management and oversight bodies should consider needs specific to privacy (e.g. internal or external resources with specialized knowledge, skills, abilities and training on privacy issues).

5.4.5 Establishing communication and consultation

The guidance in ISO 31000:2018, 5.4.5 applies.

5.5 Implementation

The guidance in ISO 31000:2018, 5.5 applies.

5.6 Evaluation

The guidance in ISO 31000:2018, 5.6 applies.

5.7 Improvement

5.7.1 Adapting

The guidance in ISO 31000:2018, 5.7.1 applies.

5.7.2 Continually improving

The guidance in ISO 31000:2018, 5.7.2 applies.

6 Risk management process

6.1 General

The guidance in ISO 31000:2018, 6.1 applies.

6.2 Communication and consultation

The guidance in ISO 31000:2018, 6.2 and the following additional guidance applies.

In the context of organizational privacy risk management processes, the following are examples of groups or individuals that can be consulted/communicated with:

— privacy experts;

— persons in charge of privacy matters;

— product and system designers and developers, for goods and services that handle PII;

— PII processing system owners;

— officers or management responsible for PII processing activities and decisions;

— supervisory authorities;

— PII principals or groups of PII principals (e.g. organizations or associations).

Some jurisdictions mandate particular types of consultations for some instances of PII processing, such as consultation of supervisory authorities. In such cases, the organization should identify its obligations for consultations and demonstrate that it complies with them in a timely manner.

6.3 Scope, context and criteria

6.3.1 General

The guidance in ISO 31000:2018, 6.3.1 applies.

6.3.2 Defining the scope

The guidance in ISO 31000:2018, 6.3.2 and the following additional guidance applies.

The scope of the organizational privacy risk management process should include:

— PII processing;

— products and services that can be used to process PII.

Where an organization implements a PIMS, the scope of the risk assessment should reflect that of the defined scope of the management system (ISO/IEC 27701:2019, 5.2.3).

6.3.3 External and internal context

The guidance in ISO 31000:2018, 6.3.3 and the following additional guidance applies.

Organizational factors can be a source of risk and can have consequences for the organization without adversely affecting individuals (e.g. a public statement about privacy from top management that may affect perceptions of the organization).

6.3.4 Defining risk criteria

The guidance in ISO 31000:2018, 6.3.4 and the following additional guidance applies.

The organization should define the risk criteria that guide the outcomes of the risk assessment results. This may include what types of measures are used (qualitative vs. quantitative), the formula or methods used to determine the risk, and the management actions for levels of risk.

In relation to organizational privacy risk, these criteria should include how privacy impact on individuals will be defined and measured, as well as how the privacy impact on individuals' factors into the organization's overall risk calculation. Furthermore, risk-based assessments of factors influencing the organization directly due to adverse privacy events that do not have impacts on PII principals, should also be considered (Annex B provides some examples of privacy events in Table B.1 and causes of privacy events in Table B.2). Potential criteria to be defined for organizational privacy risk should include:

— how organizational consequences will be defined and measured;

— how privacy impact on individuals will be defined and measured;

— positive or negative consequences for the organization;

— positive and negative privacy impacts to PII principals.

In order to help with the decision process, the risk evaluation criteria should consider the necessary balance between:

— opportunities for the organization;

— risks to the organization (consequences regarding the following reputation, fines, trials);

— risks to PII principals (privacy impacts on physical, material, non-material aspects).

For example, there can be a business opportunity that leads the organization to process new PII, with a very low risk for PII principals, but a very high reputational risk to the organization.

Table C.1 provides examples of privacy impacts to individuals.

NOTE ISO 31000 notes that risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood. In this document, "consequences" refers to consequences to the organization, while "privacy impact" refers to the impact on PII principals.

6.4 Risk assessment

6.4.1 General

The guidance in ISO 31000:2018, 6.4.1 applies.

6.4.2 Risk identification

6.4.2.1 General

The guidance in ISO 31000:2018, 6.4.2 and the following additional guidance applies.

There are a number of approaches for identifying risks in an organization. Two common ones are the event-based approach and the asset-based approach. Organizations can utilize elements of both approaches to fit their operational context. 6.4.2 outlines the elements necessary for risk identification related to the processing of PII, as well as details on the event-based and asset-based approaches.

6.4.2.2 Identification of PII processing

The organization should identify PII processing that falls within the scope of the risk management process as defined in 6.3.2, including potential PII processing by products and services. Understanding PII processing and its relative criticality and value is integral to identifying risks and assessing the privacy impact on individuals and the consequences for the organization.

Organizational privacy risk management has the following considerations when identifying PII processing:

a) PII processing activities (or types of PII processing activities) and PII processed (or types of PII);

b) the assets on which they rely;

c) categories of individuals whose PII is being processed (e.g. customers, employees);

d) purposes of the PII processing;

e) individuals or personnel processing PII;

f) role of internal and external entities engaged in the PII processing.

For evaluation of PII processing and the relation to privacy impact and consequences, see 6.4.2.7 and 6.4.3.3. For examples of considerations related to the identification of PII processing, see Annex A.

6.4.2.3 Event-based approach

6.4.2.3.1 General

An event-based approach to identifying risks is a high-level examination of risk sources and the potential scenarios that can play out based on those risk sources. Scenarios should be built by identifying the different paths, within the system, that risk sources can use to reach the PII processing, the PII, and their target objectives.

6.4.2.3.2 Identification of privacy events

As part of an event-based approach, the organization should identify (potential) privacy events in order to construct scenarios that help to identify risks. Privacy events may originate from the context within which the PII processing takes place, and involve people, processes, and technology.

Common privacy events can often be found in catalogues or can be identified through interviews with internal stakeholders, such as asset owners and employees with privacy responsibilities. Privacy events that adversely affect the organization should be described by identifying the different stakeholders and how the event affects them or is perceived by them.

Scenarios that help to identify privacy risks can be built by deduction by asking the following question:

— Given the PII processing identified in 6.4.2.2, what contextual considerations can exist that can affect a privacy event?

Examples of privacy events and their causes are described in Annex B, and contextual considerations that can affect a privacy event are described in Annex D.

NOTE Privacy events can have consequences for the organization even in the absence of adverse impacts on PII principals.

6.4.2.4 Asset-based approach

6.4.2.4.1 General

An asset-based approach to risk identification involves looking closely at organizational assets and identifying threats and vulnerabilities that can affect those assets.

Examining assets, along with potential threats and vulnerabilities, can help the organization with a more detailed and targeted risk identification process.

Scenarios can be built by identifying the different paths within the systems and data flows (on which the PII and PII processing activities rely), that risk sources can use to reach the PII processing, the PII, and their target objectives.

6.4.2.4.2 Identification of PII processing assets

To accurately identify risks via asset-based scenarios, the organization should identify assets related to PII processing. Assets can include, but are not limited, to:

— the PII itself;

— systems, software applications, databases and firmware that process PII;

— hardware used by systems that process PII (client, servers, mobile computing devices, IoT devices, external and portable memory devices, etc.);

— organizational attributes, such as reputation, that can be damaged by an adverse privacy event.

Once assets are identified, the organization can consider threats and vulnerabilities, both of which can be related to or originate from:

— the organization itself;

— processes and procedures;

— management routines;

— personnel;

— system configuration;

— technical or organizational measures or lack thereof;

— hardware, software, or services;

— external parties;

— physical environment (e.g. physical archives, physical documents);

— hardware, software, or services (e.g. websites, email).

NOTE Common information security-related vulnerabilities are described in ISO/IEC 27005.

6.4.2.5 Identification of existing controls

The organization should identify controls relevant to processing PII. Controls may be previously documented (in internal systems, procedures, audit reports, etc.) or identified during the risk management activities. Those organizations implementing a PIMS can also refer to the controls selected as part of the required statement of applicability.

6.4.2.6 Identification of biases, assumptions and beliefs

The organization should identify and evaluate the biases, assumptions, and beliefs of those involved with the PII processing or design of products and services that process PII, as well as how these can affect the data analytic inputs and outputs used in PII processing.

6.4.2.7 Identification of privacy impacts and consequences

As part of organizational privacy risk management, the organization should identify privacy impacts on individuals whose PII is being processed, as well as consequences to the organization itself. Impacts or consequences are the results of a privacy event.

Consequences for the organization necessarily differ from those of privacy impacts to individuals. Consequences to organizations can be, for example:

— investigation and repair time;

— customer abandonment of products or services;

— harm to internal organizational culture;

— (work)time lost;

— opportunity lost;

— financial cost of specific skills to repair the damage;

— impairment of image reputation, and goodwill;

— regulatory fines;

— loss of physical assets.

Privacy impacts on individuals are an externality for the organization. Therefore, it can be difficult for the organization to exactly estimate the impact on each individual. Rather than specifying each type of impact, this can be considered generally as an impact on an individual's privacy, with the degree of impact being the critical element (see 6.4.3.3 and Annex D). Organizations that perform privacy impact assessments as part of a PIMS or to comply with regulatory or legal requirements can utilize these for help in identifying the privacy impacts.

Annex C provides examples of privacy impacts in Table C.1 and consequences in Table C.2.

6.4.3 Risk analysis

6.4.3.1 General

The guidance in ISO 31000:2018, 6.4.3 and the following additional guidance applies.

6.4.3.2 Risk analysis approaches

Risk analysis approaches typically include a risk analysis process, a risk model, and an analytic approach.

A risk analysis process describes the steps for carrying out a risk analysis (e.g. prepare for the analysis, conduct the analysis, communicate analysis and results, and maintain the analysis).

A risk model defines the risk factors (e.g. threats, impacts, consequences, vulnerabilities, controls) to be assessed and the relationships among those factors. If not using a pre-defined risk model, the organization defines which risk factors will be assessed and the relationships among them.

An analytic approach includes the analysis type (i.e. quantitative, qualitative, semiquantitative) and analysis approach (i.e. threat-oriented, asset/impact-oriented, vulnerability-oriented), which help the organization determine how, with what level of detail, and in which form risk factors are to be analysed.

6.4.3.3 Assessment of privacy impact and consequence

When assessing the privacy impacts and consequences identified in the risk assessment, the organization should distinguish between an assessment of consequences to the organization and a privacy impact assessment for individuals.

Business analyses should determine the degree to which the organization can be affected by an adverse effect of PII processing or privacy events and consider elements including but not limited to:

— value (qualitative or quantitative) or criticality of product or service;

— threats, vulnerabilities, and privacy events applicable to PII processing activities;

— tangible consequences such as immediate and medium-term costs (e.g. costs for the immediate work around and for the final solution, fines);

— intangible consequences (e.g. to the brand), that can have long-term costs, loss of customers;

— criteria used to establish the overall consequence (as determined in 6.3.4);

— existing protections and mitigating controls around PII (e.g. de-identification).

Privacy consequences reflect the extent to which there can be a direct adverse effect, or cost, to the organization as a result of a privacy event.

Privacy impact reflects the degree to which PII principals can be affected by privacy events. Privacy impact analyses may be performed as part of the privacy risk assessment, or they can be standalone processes (e.g. as part of a PIMS or as required by regulation or law). The organization should consider elements such as:

— types of PII processed;

— amount of PII processed;

— use of the PII that is processed (purpose for the processing);

— protections and mitigating controls around PII (e.g. de-identification);

— jurisdictional and cultural environment of the PII principal (which can affect how the relative impact is determined).

After considering the potential impacts on PII principals and consequences for the organization, the criteria for performing the risk assessment (6.3.4) can be used to estimate the level of impact and consequence of each privacy event, in order to rank them.

An example of a scale for privacy impacts is provided in Annex D and a template for impact level in Table D.1.

6.4.3.4 Assessment of likelihood

The organization should assess the likelihood of privacy events. Likelihood can be determined on a qualitative or quantitative scale and should align to the criteria established as part of 6.3.4. Likelihood can be affected by (but not limited to):

— organizational factors (e.g. geographic location, the public perception about participating organizations with respect to privacy);

— system factors [e.g. the nature and history of individuals' interactions with the system; visibility of data processing to individuals and third parties; types, severity, and number of vulnerabilities; frequency, severity, and pervasiveness of threats; success (mitigation) or failure of controls (6.4.2.4)]; or

— individuals' factors (e.g. individuals' demographics, privacy interests or perceptions, data sensitivity).

6.4.4 Risk evaluation

The guidance in ISO 31000:2018, 6.4.4 and the following additional guidance applies.

When evaluating the results of the privacy risk analysis against the established risk criteria, the organization should consider the following when determining the response to risk:

— the degree of acceptable risk, which can vary depending on the context, including the applicable legislation;

— whether findings in the risk analysis affect the obligations to PII principals, including those mandated by applicable legislation.

6.5 Risk treatment

6.5.1 General

The guidance in ISO 31000:2018, 6.5.1 applies.

6.5.2 Selection of risk treatment options

6.5.2.1 General

The guidance in ISO 31000:2018, 6.5.2 and the following additional guidance applies.

When selecting risk treatment options, the organization should consider options not only in the context of their own organization but also in relation to the privacy of individuals. For example, if a risk is identified based on a high impact on the individual and consequence to the organization, that risk may be treated by enhanced privacy by design controls (e.g. encryption, pseudonymization), thus enhancing privacy protections for individuals, as well as protecting the organization from reputational damage or regulatory fines.

If implementing a privacy information management system (PIMS), such as in ISO/IEC 27701, the organization should use the risk treatment process to help guide the selection of controls to be included in the statement of applicability.

6.5.2.2 Risk modification

Controls can be added, removed, or modified to reduce the likelihood of risk to what is acceptable to the organization. Controls applied to privacy risk can be informed by local laws and regulations, as well as best practices. ISO/IEC 27701 provides controls that may be selected by an organization to implement a PIMS based on a risk approach.

6.5.2.3 Risk retention

Risk should only be retained if it meets the baseline criteria for risk acceptance. Those criteria should be determined by the organization based on the context.

6.5.2.4 Risk avoidance

The organization can choose to avoid an identified risk by modifying or cancelling activities (or planned activities) that create the risk. In the context of processing PII, this can include, for example, choosing not to process a particular type of PII.

6.5.2.5 Risk sharing

Risk can be shared between the organization and an external party, which can include a business partner, subcontractor, or even a customer. In the context of PII processors, for example, the processor may offer a service for which the customer has control over certain aspects of risk (e.g. whether to enable encryption or require two-factor authentication). When sharing risk, the organization should consider new or additional risks created by the external relationship.

For example, contracts are a means of sharing or transferring risk to other organizations (such as through an insurance policy).

6.5.3 Preparing and implementing risk treatment plans

The guidance in ISO 31000:2018, 6.5.3 and the following additional guidance applies.

Privacy risk treatment plans and the responsibilities for their implementation should be reviewed and approved by management.

6.6 Monitoring and review

The guidance in ISO 31000:2018, 6.6 and the following additional guidance applies.

The organization should monitor for changes that may affect privacy risk. These changes may necessitate the review of organizational privacy risk management processes and risk treatment plans for changes or improvements. The organization can monitor, for example:

— the organization's business environment (e.g. the introduction of new technologies);

— new or altered legal obligations;

— changes to risk tolerance;

— new or altered PII processing or IT systems;

— new privacy events, threats, and vulnerabilities disclosed to the organization from internal or external sources;

— continued effectiveness of planned mitigation activities;

— the decisions of the relevant supervisory authorities.

6.7 Recording and reporting

The guidance in ISO 31000:2018, 6.7 and the following additional guidance applies.

Both organizations and individuals may need to know how PII is processed in order to manage privacy risk effectively. Through internal and external reporting on PII processing, associated privacy risks, and risk treatments, the organization can increase transparency, establish a more reliable understanding of PII processing activities, and build trust.

Organizational privacy risks should be reported to top management, including a summary risk assessment and risk management report.

NOTE External reporting is usually different from internal (e.g. a summary report instead of a detailed report).

Annex A
(informative)

PII processing identification

Identifying the specific PII and processing enables an organization to more accurately assess the privacy impact on individuals and consequences to the organization itself should privacy events or threats materialize. Several key elements can be inventoried to illustrate or map out the organization's PII processing and its context to support organizational privacy risk management:

— PII processing activities (e.g. collection, storage, alteration, retrieval, consultation, disclosure, anonymization, pseudonymization, dissemination or otherwise making available, deletion, or destruction);

— types of PII (see Table A.1);

— purposes of the PII processing (see Table A.2);

— PII processing environment (e.g. geographic location, internal, cloud, third parties);

— assets on which PII processing activities rely (e.g. systems/products/services that process PII);

— categories of individuals whose PII is being processed (e.g. customers, employees, prospective employees, or consumers);

— individuals or personnel processing PII (e.g. the organization or third parties such as service providers, partners, customers, and developers);

— role of entities engaged in PII processing (e.g. internal or external).

Distinguishing types and uses of PII can help organizations further refine privacy impacts and consequences. Different data types and uses can have higher or lower relative values or sensitivity depending on the context, and organizations can choose to assign sensitivity "ratings" depending on this context. Organizations can utilize published taxonomies to assist in identifying types and uses of PII (for example, a taxonomy for cloud computing and distributed platforms is found in ISO/IEC 19944-1) or use existing classification systems internal to the organization. Table A.1 provides examples of PII data types, while Table A.2 provides example uses of PII data.

Table A.1 — Example PII data types

Examples
Civil status, identity, identification data (social security or other identification number)
Contact data (phone number, address, e-mail, etc.)
Personal life (living habits, marital status, philosophical, political, religious and trade-union views, sex life, health data, racial or ethnic origin, offences/convictions, etc. – excluding sensitive or dangerous data)
Professional life (résumé, education and professional training, awards, etc.)
Economic and financial information (bank data, income, financial situation, tax situation, etc.)
Connection data (IP addresses, event logs, etc.)
Location data (travels, GPS data, GSM data, etc.)
Credentials (PIN, passwords, knowledge-based authentication data, etc.)
Biometric data

Table A.2 — Example uses of PII data

Examples
Provide a service or product (e.g. fulfilling an order, processing a bank deposit, business process execution)
Improve a service or product (e.g. to increase the quality)
Personalize a service or product (e.g. to tailor to a particular user)
Offer upgrades/upsell a service or product (e.g. for additional products or services, or additional capabilities of existing products or services)
Market/advertise/promote a service or product
Share (e.g. share or transfer PII to one or more third-parties)
Design or develop a service or product
Develop data models or train AI systems
Prevent fraud