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

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.