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/IEC 2022



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2022

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

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

Published in Switzerland

© ISO/IEC 2022 – All rights reserved

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Principles of organizational privacy risk management ... **2**
5 Framework ... **2**
5.1 General ... 2
5.2 Leadership and commitment ... 2
5.3 Integration ... 3
5.4 Design ... 3
5.4.1 Understanding the organization and its context ... 3
5.4.2 Articulating risk management commitment ... 3
5.4.3 Assigning organizational roles, authorities, responsibilities and accountabilities ... 3
5.4.4 Allocating resources ... 3
5.4.5 Establishing communication and consultation ... 4
5.5 Implementation ... 4
5.6 Evaluation ... 4
5.7 Improvement ... 4
5.7.1 Adapting ... 4
5.7.2 Continually improving ... 4
6 Risk management process ... **4**
6.1 General ... 4
6.2 Communication and consultation ... 4
6.3 Scope, context and criteria ... 5
6.3.1 General ... 5
6.3.2 Defining the scope ... 5
6.3.3 External and internal context ... 5
6.3.4 Defining risk criteria ... 5
6.4 Risk assessment ... 6
6.4.1 General ... 6
6.4.2 Risk identification ... 6
6.4.3 Risk analysis ... 9
6.4.4 Risk evaluation ... 10
6.5 Risk treatment ... 10
6.5.1 General ... 10
6.5.2 Selection of risk treatment options ... 10
6.5.3 Preparing and implementing risk treatment plans ... 11
6.6 Monitoring and review ... 11
6.7 Recording and reporting ... 12
Annex A (informative) **PII processing identification** ... **13**
Annex B (informative) **Example privacy events and causes** ... **15**
Annex C (informative) **Privacy impact and consequence examples** ... **17**
Annex D (informative) **Template showing the severity scale for privacy impacts on individuals** ... **18**
Bibliography ... **19**

© ISO/IEC 2022 – All rights reserved

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.

© ISO/IEC 2022 – All rights reserved

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.

© ISO/IEC 2022 – All rights reserved

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/

© ISO/IEC 2022 – All rights reserved

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;

© ISO/IEC 2022 – All rights reserved