International Standard

ISO/IEC 27554

First edition
2024-07

Information security, cybersecurity and privacy protection — Application of ISO 31000 for assessment of identity-related risk

Reference number
ISO/IEC 27554:2024(en)

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).

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*.

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

ISO 31000 provides guidelines and a methodology for assessing risk. The additional guidance provided in this document supports the use of ISO 31000:2018 in the field of identity management, in particular for the risk management for identities. This document elaborates on the steps in the methodology provided in ISO 31000, demonstrating how to apply them to the assessment of identity-related risk. Therefore, this document is an application of ISO 31000 for the assessment of identity-related risk. This document is intended to be used in connection with ISO 31000:2018.

While the contexts in which identities are established differ between implementations, there are some elements that are consistent. This document presents those elements where they have been identified.

This document is intended to help organizations establishing and using identities to understand the risks posed by these identities, in order to determine what is needed to mitigate these risks. The manner in which this is done enables the output of the assessment process to be used as an input into processes which are described in other identity management standards, where a risk-based approach is specified for determining levels of assurance.

Information security, cybersecurity and privacy protection — Application of ISO 31000 for assessment of identity-related risk

1 Scope

This document provides guidelines for identity-related risk, as an extension of ISO 31000:2018. More specifically, it uses the process outlined in ISO 31000 to guide users in establishing context and assessing risk, including providing risk scenarios for processes and implementations that are exposed to identity-related risk.

This document is applicable to the risk assessment of processes and services that rely on or are related to identity. This document does not include aspects of risk related to general issues of delivery, technology or security.

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*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 31000 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
risk identification
process of finding, recognizing and describing risks

Note 1 to entry: Risk identification involves the identification of risk sources, events, their causes and their potential consequences.

Note 2 to entry: Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and interested parties' needs.

[SOURCE: ISO 31073:2022, 3.3.9]

3.2
risk analysis
process to comprehend the nature of risk and to determine the *level of risk* (3.5)

Note 1 to entry: Risk analysis provides the basis for risk evaluation and decisions about risk treatment.

Note 2 to entry: Risk analysis includes risk estimation.

[SOURCE: ISO 28002:2011, 3.51]

3.3
risk evaluation
process of comparing the results of *risk analysis* (3.2) with risk criteria to determine whether the risk is acceptable or tolerable

Note 1 to entry: Risk evaluation assists in the decision about *risk treatment* (3.6).

[SOURCE: ISO 31073:2022, 3.3.25]

3.4
risk assessment
overall process of *risk identification* (3.1), *risk analysis* (3.2) and *risk evaluation* (3.3)

[SOURCE: ISO 31073:2022, 3.3.8]

3.5
level of risk
magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood

[SOURCE: ISO 31073:2022, 3.3.22]

3.6
risk treatment
process to modify risk

Note 1 to entry: Risk treatment can involve:

— avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;

— taking or increasing risk in order to pursue an opportunity;

— removing the risk source;

— changing the likelihood;

— changing the consequences;

— sharing the risk with another party or parties (including contracts and risk financing); and

— retaining the risk by informed choice.

Note 2 to entry: Risk treatments that deal with negative consequences are sometimes referred to as “risk mitigation”, “risk elimination”, “risk prevention” and “risk reduction”.

Note 3 to entry: Risk treatment can create new risks or modify existing risks.

[SOURCE: ISO 31073:2022, 3.3.32]

3.7
risk control
measure that maintains and/or modifies risk

Note 1 to entry: Risk controls include, but are not limited to, any process, policy, device, practice, or other conditions and/or actions which maintain and/or modify risk.

Note 2 to entry: Risk controls do not always exert the intended or assumed modifying effect.

[SOURCE: ISO 31073:2022, 3.3.33]

3.8
identity
partial identity
set of attributes related to an entity

Note 1 to entry: An entity can have more than one identity.

Note 2 to entry: Several entities can have the same identity.

[SOURCE: ISO/IEC 24760-1:2019, 3.1.2, modified — "partial identity" has been changed to an admitted term; Note 3 to entry has been removed.]

3.9
identity information
set of values of attributes optionally with any associated metadata in an identity

Note 1 to entry: In an information and communication technology system an identity is present as identity information.

[SOURCE: ISO/IEC 24760-1:2019, 3.2.4]

3.10
identity management
processes and policies involved in managing the lifecycle and value, type and optional metadata of attributes in identities known in a particular domain

Note 1 to entry: In general identity management is involved in interactions between parties where identity information is processed.

Note 2 to entry: Processes and policies in identity management support the functions of an identity information authority where applicable, in particular to handle the interaction between an entity for which an identity is managed and the identity information authority.

[SOURCE: ISO/IEC 24760-1:2019, 3.4.1]

3.11
identity theft
result of a successful false claim of identity

[SOURCE: ISO/IEC 24760-3:2016, 3.4]

4 Principles

The principles presented in ISO 31000:2018, Clause 4 also apply when assessing identity-related risk.

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 applies.

5.3 Integration

The guidance in ISO 31000:2018, 5.3 applies.

5.4 Design

The guidance in ISO 31000:2018, 5.4 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

The guidance in ISO 31000:2018, 5.7 applies.

6 Process

6.1 General

The guidance in ISO 31000:2018, 6.1 applies. Figure 1 below is an adaptation of ISO 31000:2018, Figure 1, which illustrates the risk management process.

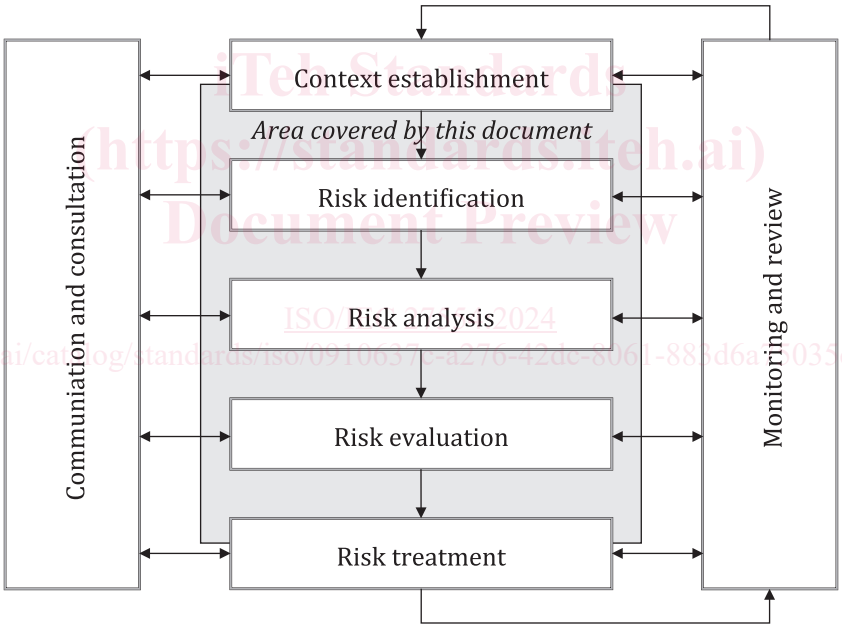

Figure 1 — Risk management process

6.2 Communication and consultation

The guidance in ISO 31000:2018, 6.2 applies.

6.3 Scope, context and criteria

The guidance in ISO 31000:2018, 6.3 applies.

6.4 Risk assessment

The guidance in ISO 31000:2018, 6.4 applies.