International Standard

ISO/IEC 27554

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

First edition
2024-07

Reference number
ISO/IEC 27554:2024(en)

© ISO/IEC 2024



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 ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Principles ... **3**
5 Framework ... **3**
5.1 General ... 3
5.2 Leadership and commitment ... 3
5.3 Integration ... 3
5.4 Design ... 4
5.5 Implementation ... 4
5.6 Evaluation ... 4
5.7 Improvement ... 4
6 Process ... **4**
6.1 General ... 4
6.2 Communication and consultation ... 4
6.3 Scope, context and criteria ... 4
6.4 Risk assessment ... 4
6.5 Risk treatment ... 5
6.6 Monitoring and review ... 5
6.7 Recording and reporting ... 5
7 Identity-related context establishment ... **5**
7.1 General ... 5
7.2 Actors ... 5
7.2.1 Subscribers/Actors ... 5
7.2.2 Administrators ... 5
7.3 Types of personal data ... 5
7.4 Policies and regulations ... 5
7.5 Service and transaction scope ... 5
8 Identity-related risk assessment ... **6**
9 Identity-related risk identification ... **6**
10 Identity-related risk analysis ... **7**
10.1 General ... 7
10.2 Affected parties ... 7
10.3 Identity theft or fabrication ... 7
10.4 Categories of consequences of identity-related risk ... 8
10.5 Risk impact assessment ... 8
11 Identity-related risk evaluation ... **9**
12 Identity-related risk treatment ... **9**
Annex A (informative) **Standards related to identity-management risk assessment** ... **10**
Annex B (informative) **Risk impact assessment** ... **13**
Bibliography ... **18**

© ISO/IEC 2024 – 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).

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.

© ISO/IEC 2024 – All rights reserved

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.

© ISO/IEC 2024 – All rights reserved

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]

© ISO/IEC 2024 – All rights reserved