

Date: 2023-10-29

ISO/IEC ~~DIS~~PRF 27554:2023(E)

ISO/IEC JTC 1/SC 27/WG 5

Secretariat: DIN

Date: 2024-04-25

Information security, cybersecurity and privacy protection — Application of ISO 31000 for

assessment of identity-related risk

iTeh Standards  
(<https://standards.iteh.ai>)

FDIS stage Document Preview

[ISO/IEC PRF 27554](https://standards.iteh.ai/catalog/standards/iso/0910637c-a276-42dc-8061-883d6a75035c/iso-iec-prf-27554)

<https://standards.iteh.ai/catalog/standards/iso/0910637c-a276-42dc-8061-883d6a75035c/iso-iec-prf-27554>

Edited DIS - MUST BE USED FOR FINAL DRAFT

Style Definition

Formatted: Left: 1.5 cm, Right: 1.5 cm, Section start: New page, Header distance from edge: 1.27 cm, Footer distance from edge: 1.27 cm, Numbering: Restart each page

Formatted: Font: 14 pt, English (United Kingdom)

Formatted: zzCover large

Formatted

Formatted

Formatted: Cover Title\_A1

© ISO/IEC 2023/2024

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

Tel. +41 22 749 01 11

Fax +41 22 749 09 47

E-mail: [copyright@iso.org](mailto:copyright@iso.org)

Web: [www.iso.org](http://www.iso.org)

Website: [www.iso.org](http://www.iso.org)

Published in Switzerland.

Formatted: Font: 11 pt

Formatted: HeaderCentered, Space After: 0 pt, Line spacing: single

Formatted: Font: 11 pt

Formatted: Font: 11 pt

Formatted: No page break before, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Default Paragraph Font

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: French (Switzerland)

Formatted: French (Switzerland)

Formatted: French (Switzerland)

Formatted: zzCopyright address, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: French (Switzerland)

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

iTeh Standards  
(<https://standards.itih.ai>)  
Document Preview

ISO/IEC PRF 27554

<https://standards.itih.ai/catalog/standards/iso/0910637c-a276-42dc-8061-883d6a75035c/iso-iec-prf-27554>

Formatted: FooterPageRomanNumber

Formatted: Font: 11 pt  
Formatted: Font: 11 pt  
Formatted: HeaderCentered, Left, Space After: 0 pt, Line spacing: single  
Formatted: Font: 11 pt

iTeh Standards  
(<https://standards.iteh.ai>)  
Document Preview

ISO/IEC PRF 27554

<https://standards.iteh.ai/catalog/standards/iso/0910637c-a276-42dc-8061-883d6a75035c/iso-iec-prf-27554>

Formatted: FooterPageRomanNumber

Formatted: Font: 11 pt  
Formatted: HeaderCentered, Space After: 0 pt, Line spacing: single  
Formatted: Font: 11 pt  
Formatted: Font: 11 pt

Contents

Foreword .....5  
Introduction .....6  
1 Scope .....7  
2 Normative references .....7  
3 Terms and definitions .....7  
4 Principles .....10  
5 Framework .....11  
6 Process .....11  
7 Identity-related risk assessment .....11  
8 Identity-related context establishment .....11  
8.1. General .....11  
8.2. Actors .....12  
8.2.1 Subscribers/Actors .....12  
8.2.2 Administrators .....12  
8.3. Types of personal data .....12  
8.4. Policies & regulations .....12  
8.5. Service and transaction scope .....12  
9. Identity-related risk identification .....13  
10. Identity-related risk analysis .....13  
10.1 General .....13  
10.2 Affected parties .....14  
10.3 Identity theft or fabrication .....14  
10.4 Categories of consequences of identity-related risk .....14  
10.5 Risk impact assessment .....15  
11. Identity-related risk evaluation .....15  
12. Identity-related risk treatment .....16  
Annex A (informative) Standards for identity management risk assessment .....17  
A.1 Standards guidance on risk management .....17  
A.2 Standards guidance on identity management .....17  
Annex B (informative) Risk impact assessment .....20  
B.1 Assessing the degree of impact of a consequence .....20  
B.2 Assigning levels to the assessed impact .....20  
B.3 Impact level guide .....21  
B.4 Control selection and effectiveness .....23  
B.5 Likelihood assessment .....24

Formatted: FooterPageRomanNumber

**B.6 Plotting level of risk ..... 24**

**Foreword ..... vii**

**Introduction ..... viii**

**1 Scope ..... 1**

**2 Normative references ..... 1**

**3 Terms and definitions ..... 1**

**4 Principles ..... 4**

**5 Framework ..... 4**

**5.1 General ..... 4**

**5.2 Leadership and commitment ..... 4**

**5.3 Integration ..... 4**

**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 ..... 5**

**6.3 Scope, context and criteria ..... 5**

**6.4 Risk assessment ..... 5**

**6.5 Risk treatment ..... 5**

**6.6 Monitoring and review ..... 6**

**6.7 Recording and reporting ..... 6**

**7 Identity-related context establishment ..... 6**

**7.1 General ..... 6**

**7.2 Actors ..... 6**

**7.2.1 Subscribers/Actors ..... 6**

**7.2.2 Administrators ..... 7**

**7.3 Types of personal data ..... 7**

**7.4 Policies and regulations ..... 7**

**7.5 Service and transaction scope ..... 7**

**8 Identity-related risk assessment ..... 8**

**9 Identity-related risk identification ..... 8**

**10 Identity-related risk analysis ..... 9**

**10.1 General ..... 9**

**10.2 Affected parties ..... 9**

**10.3 Identity theft or fabrication ..... 9**

**10.4 Categories of consequences of identity-related risk ..... 10**

**10.5 Risk impact assessment ..... 10**

**11 Identity-related risk evaluation ..... 11**

**12 Identity-related risk treatment ..... 12**

**Annex A (informative) Standards related to identity-management risk assessment ..... 13**

**A.1 Standards related to risk management guidance ..... 13**

**A.1.1 Risk management guidance defined in ISO 31000:2018 ..... 13**

Formatted: Font: 11 pt

Formatted: Font: 11 pt

Formatted: HeaderCentered, Left, Space After: 0 pt, Line spacing: single

Formatted: Font: 11 pt

Formatted: FooterPageRomanNumber

**A.1.2 Risk assessment techniques defined in IEC 31010:2019..... 13**  
**A.2 Standards on identity management guidance ..... 13**  
**A.2.1 Identity management framework defined in ISO/IEC 24760..... 13**  
**A.2.2 Identity proofing defined in ISO/IEC TS 29003 ..... 14**  
**A.2.3 Entity authentication described in ISO/IEC 29115..... 14**  
**A.2.4 Authorization/access control described in ISO/IEC 29146 ..... 14**  
**A.2.5 Trust anchors for DLT-based identity management (TADIM) described in ISO/IEC 23644..... 14**  
**Annex B (informative) Risk impact assessment ..... 16**  
**B.1 Assessing the degree of impact of a consequence..... 16**  
**B.2 Assigning levels to the assessed impact ..... 17**  
**B.3 Impact level guide..... 17**  
**B.4 Control selection and effectiveness ..... 19**  
**B.5 Likelihood assessment ..... 20**  
**B.6 Plotting level of risk ..... 21**  
**Bibliography ..... 22**

Formatted: Font: 11 pt  
Formatted: HeaderCentered, Space After: 0 pt, Line spacing: single  
Formatted: Font: 11 pt  
Formatted: Font: 11 pt

iTeh Standards  
(https://standards.itih.ai)  
Document Preview

ISO/IEC PRF 27554

<https://standards.itih.ai/catalog/standards/iso/0910637c-a276-42dc-8061-883d6a75035c/iso-iec-prf-27554>

Formatted: FooterPageRomanNumber

## 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](http://www.iso.org/directives) or [www.iec.ch/members\\_experts/refdocs](http://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~~ 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](http://www.iso.org/patents) and <https://patents.iec.ch> ~~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](http://www.iso.org/iso/foreword.html). In the IEC, see [www.iec.ch/understanding-standards](http://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](http://www.iso.org/members.html) and [www.iec.ch/national-committees](http://www.iec.ch/national-committees).

Formatted: Font: 11 pt

Formatted: Font: 11 pt

Formatted: HeaderCentered, Left, Space After: 0 pt, Line spacing: single

Formatted: Font: 11 pt

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: English (United Kingdom)

Field Code Changed

Formatted: Font: Not Italic, Font color: Auto

Formatted: English (United Kingdom)

Field Code Changed

Formatted: FooterPageRomanNumber

## 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.

- Formatted: Font: 11 pt
- Formatted: HeaderCentered, Space After: 0 pt, Line spacing: single
- Formatted: Font: 11 pt
- Formatted: Font: 11 pt
- Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers
- Formatted: Default Paragraph Font
- Formatted: Default Paragraph Font
- Formatted: Default Paragraph Font
- Formatted: Default Paragraph Font

# iTeh Standards (<https://standards.iteh.ai>) Document Preview

ISO/IEC PRF 27554

<https://standards.iteh.ai/catalog/standards/iso/0910637c-a276-42dc-8061-883d6a75035c/iso-iec-prf-27554>



# 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)(3.5)

Formatted: Font: 16 pt

Formatted: Default Paragraph Font, Font: 16 pt

Formatted: Font: 16 pt

Formatted: Default Paragraph Font, Font: 16 pt

Formatted: Font: 16 pt

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Default Paragraph Font

Formatted: Default Paragraph Font

Formatted: Default Paragraph Font

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers, Tab stops: Not at 0.7 cm + 1.4 cm + 2.1 cm + 2.8 cm + 3.5 cm + 4.2 cm + 4.9 cm + 5.6 cm + 6.3 cm + 7 cm

Formatted: Default Paragraph Font

Formatted: Default Paragraph Font

Formatted: Default Paragraph Font, Font: Italic

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: English (United Kingdom)

Formatted: Font: Cambria, 11 pt, English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: Font: Cambria, English (United Kingdom)

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Font: Not Italic

Formatted: Line spacing: At least 11 pt, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers, Tab stops: Not at 0.7 cm + 1.4 cm + 2.1 cm + 2.8 cm + 3.5 cm + 4.2 cm + 4.9 cm + 5.6 cm + 6.3 cm + 7 cm

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Default Paragraph Font

Formatted: Default Paragraph Font

Formatted: Default Paragraph Font

Formatted: Font: Not Italic

Formatted: Font: Not Italic

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 Guide 73:2009/28002:2011, 3.6.151]

3.3 risk evaluation

process of comparing the results of risk analysis (3.2)(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)(3.1), risk analysis (3.2)(3.2) and risk evaluation (3.3)(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]

Formatted: Font: 11 pt
Formatted: Font: 11 pt
Formatted: HeaderCentered, Space After: 0 pt, Line spacing: single
Formatted: Font: 11 pt
Formatted: Line spacing: At least 11 pt, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers, Tab stops: Not at 0.7 cm + 1.4 cm + 2 cm + 2.1 cm + 2.8 cm + 3.5 cm + 4.2 cm + 4.9 cm + 5.6 cm + 6.3 cm + 7 cm
Formatted: Default Paragraph Font
Formatted: Default Paragraph Font
Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers
Formatted: Font: Not Italic
Formatted: Line spacing: At least 11 pt, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers, Tab stops: Not at 0.7 cm + 1.4 cm + 2 cm + 2.1 cm + 2.8 cm + 3.5 cm + 4.2 cm + 4.9 cm + 5.6 cm + 6.3 cm + 7 cm
Formatted: Font: Italic
Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers
Formatted: Default Paragraph Font
Formatted: Default Paragraph Font
Formatted: Font: Not Italic
Formatted: Font: Not Italic
Formatted: Default Paragraph Font
Formatted: Default Paragraph Font
Formatted: Default Paragraph Font
Formatted: Font: Not Italic
Formatted: Font: Not Italic
Formatted: Default Paragraph Font
Formatted: Default Paragraph Font
Formatted: Default Paragraph Font
Formatted: Font: Not Italic
Formatted: Font: Not Italic
Formatted: Default Paragraph Font
Formatted: Default Paragraph Font
Formatted: Default Paragraph Font
Formatted: Font: Not Italic
Formatted: Font: Not Italic
Formatted: Default Paragraph Font
Formatted: Default Paragraph Font
Formatted: Default Paragraph Font
Formatted: Default Paragraph Font
Formatted: FooterPageRomanNumber

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]

Formatted: Font: 11 pt
Formatted: HeaderCentered, Left, Space After: 0 pt, Line spacing: single
Formatted: Font: 11 pt
Formatted: Font: 11 pt

Formatted

Formatted: Default Paragraph Font
Formatted: Default Paragraph Font
Formatted: Default Paragraph Font
Formatted: Default Paragraph Font
Formatted: English (United Kingdom)
Formatted
Formatted: Regular, Font: Bold
Formatted
Formatted: Default Paragraph Font
Formatted: Default Paragraph Font
Formatted: Default Paragraph Font
Formatted: Default Paragraph Font
Formatted: Default Paragraph Font
Formatted: Default Paragraph Font
Formatted: Default Paragraph Font

Formatted
Formatted

Formatted: English (United Kingdom)
Formatted
Formatted
Formatted: English (United Kingdom)
Formatted
Formatted: English (United Kingdom)
Formatted
Formatted: English (United Kingdom)
Formatted
Formatted: English (United Kingdom)
Formatted
Formatted: English (United Kingdom)
Formatted
Formatted: English (United Kingdom)
Formatted

Formatted: English (United Kingdom)
Formatted
Formatted: English (United Kingdom)
Formatted
Formatted: Default Paragraph Font
Formatted: Default Paragraph Font
Formatted: Default Paragraph Font
Formatted: Default Paragraph Font
Formatted: FooterPageRomanNumber