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)

COPYRIGHT PROTECTED DOCUMENT

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.

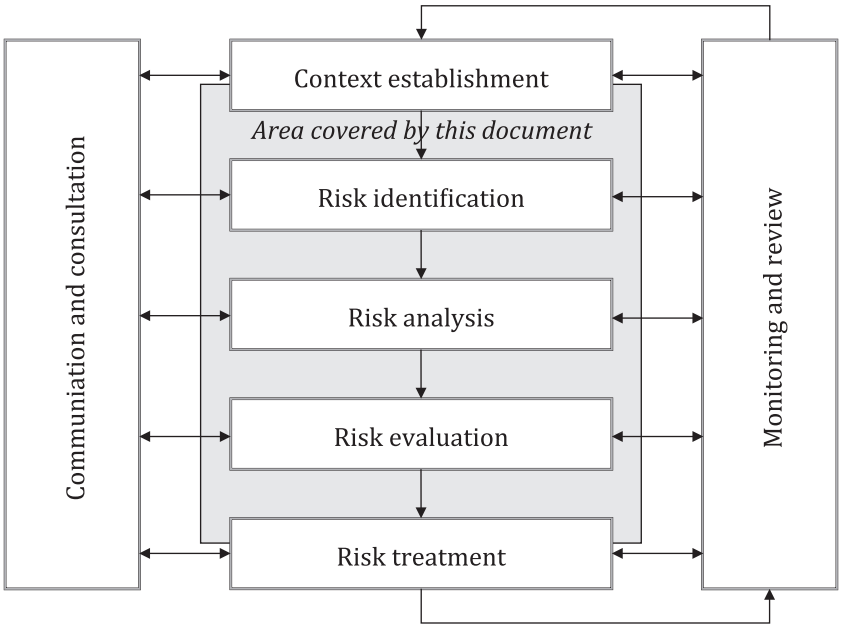

Figure 1 — Risk management process

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.

6.5 Risk treatment

The guidance in ISO 31000:2018, 6.5 applies.

6.6 Monitoring and review

The guidance in ISO 31000:2018, 6.6 applies.

6.7 Recording and reporting

The guidance in ISO 31000:2018, 6.7 applies.

7 Identity-related context establishment

7.1 General

Risk assessment is conducted in a given context. This clause identifies elements of the organization and organizational systems that have particular relevance for identity-related risk assessment. See Annex A for standards related to identity-management risk assessment.

7.2 Actors

7.2.1 Subscribers/Actors

Identifying and understanding service or transaction actors is foundational for being able to identify and classify specific risks. Actors can be categorised in multiple distinct ways, for example: internal or external to the organization; having special privileges or none. Organizations should also consider whether the identified actors are bound by any contractual, legal, or other types of agreements.

7.2.2 Administrators

For the purposes of identity-related risk assessment of a service or transaction, administrators are a group of users. Nonetheless, privileged administrators, with responsibility for parts of the identity management lifecycle, or with privileged system access that allows them to intervene in the identity management system, are treated as a separate group of actors in the assessment of identity-related risk.

7.3 Types of personal data

Identifying the types of data that are stored and processed, and determining the specific risks, are precursors to determining the target assurance levels. Data can be grouped using several distinct dimensions, for example:

— sector-specific: financial, medical;

— sensitivity: personally identifiable information, other protected types;

— availability: public, confidential, secret.

7.4 Policies and regulations

Whether or not an organization or its transactions is subject to policy or regulatory requirements, the latter affects its risk profile.

7.5 Service and transaction scope

In addition to the overall context, an organization should determine and document the scope of the service and each of its transactions before carrying out the identity-related risk assessment.

For the service, it is important to establish:

— the various roles of individuals within the service;

— the value of the service to the organization;

— what the service offers now (current transactions) and what is planned in the future.

The following should be determined for each transaction to be assessed:

— individual roles that have access within the transaction;

— prerequisites for accessing the transaction, other than registration;

— how the transaction is initiated;

— information collected and stored for the transaction;

— direct outcomes of the transaction;

— information that becomes accessible;

— actions that can be carried out;

— financial implications;

— other forms of entitlement;

— intervention points in the process (end point of the transaction);

— events or other transactions directly triggered by the transaction being assessed;

— other services or transactions that become accessible as a result of completing the transaction;

— periodic assessment of gained access;

— time-bound access based on the current service/transaction.

8 Identity-related risk assessment

This document also uses the process outlined in ISO 31000 to give guidelines for establishing context and assessing risk, including providing risk scenarios for processes and implementations that are exposed to identity-related risk.

9 Identity-related risk identification

Identity-related risk arises from the threat posed by identity theft and fabrication within a service or transaction. These are realized as identity crime, which describes the gaining of money, goods, services, or other benefits, or the avoidance of obligations through the use of a fabricated or stolen/assumed identity. Identity-related risks also arise from permitted impersonation, where an identity owner colludes with another who uses that identity falsely.

Identity-related risk is very specific and is expressed by the following two risks:

a) Risk 1: incorrect information is provided for a service or transaction.

This is the risk of providing or denying a service or transaction to a person, based on someone giving incorrect information during enrolment for, or later use of, a service or transaction.

b) Risk 2: someone is incorrectly linked to or associated with the information or authenticator used in a service or transaction.

This is the risk that by using someone else's information or authenticator, a person can gain an advantage they are not entitled to, avoid obligations such as paying fines, or impact the entitlement of someone else.

Other activities which are not considered as identity-related risk include:

— internal fraud – where staff deliberately undermine the system and its processes;

— collusion – where an individual deliberately gives away their identity or access;

— hacking – where skilled people circumvent a (computer) system's security to access records, usually involving information of multiple individuals;

— identity loss – where identity information has been lost (accidentally or otherwise) but is not used for fraudulent purposes.

Organizations should have other strategies in place to deal with the risks associated with these activities.

10 Identity-related risk analysis

10.1 General

Risk analysis involves developing a better understanding of the risk and provides an input to risk evaluation. It involves consideration of who can be affected, the identity theft and fabrication sources, the consequences associated with each risk and what the impact of risks can be.

10.2 Affected parties

As part of identity-related risk analysis, it is useful to understand who is affected by the consequences of identity-related risk. The affected parties are:

— Entitled individuals

EXAMPLE 1 An entitled individual applies for a service and is deemed ineligible because their identity has been used previously by someone else to claim the same service.

— Service providers

EXAMPLE 2 An organization's reputation suffers as a result of publicity revealing that the agency has been defrauded by large numbers of individuals claiming false identities.

— The wider community

EXAMPLE 3 Identity-related documents are mistakenly issued to people with false identities and are then used to commit fraud against other organizations.

10.3 Identity theft or fabrication

Identity theft or fabrication can cause someone financial loss, damage to reputation, physical or emotional harm, or embarrassment. In order to help determine which consequences apply and the degree of impact they can impose, it is helpful to consider both the motivation behind identity theft or fabrication and who can perpetrate these actions.

Table 1 provides examples of significant motives and some of the parties that are likely to carry out identity theft or fabrication.

Table 1 — Motives and parties

Motives	Motive description	Parties
Gain	Most commonly, the motive is financial, but it can also be in order to acquire goods or access services or information provided by the transaction.	People who wish to benefit inappropriately from the good, service or transaction (e.g. other customers, scammers).
Personal attack	Financial loss, damage to reputation, physical harm, embarrassment.	People with a grudge against the individual (e.g. ex-partners, colleagues, competitors). People with a grudge against the service provider (e.g. competitors, former employees).
Misrepresentation	Using someone else's identity and associated qualifications, reputation etc. to carry out an activity the perpetrator would not otherwise be able to.	People with a particular agenda (e.g. competitors, egotists, terrorists, criminals).
Nuisance	This motive is less likely to target a specific individual and does not carry the intention of harm that revenge does.	People with no particular agenda, can be bored or just out to cause trouble.

10.4 Categories of consequences of identity-related risk

The consequences that can arise from the identity-related risks include:

— Financial loss or liability

EXAMPLE 1 Payment of a financial benefit to an individual using a stolen or fictitious identity, who is not entitled to receive that benefit, creates a direct financial loss to the source of the funds.

— Unauthorized release of sensitive information

EXAMPLE 2 An individual's privacy rights are impinged if their personal information is released to an unauthorized party.

— Qualification/identity/reputation loss or damage

EXAMPLE 3 Use of a stolen qualification/identity results in the representation of possessing a skill/identity which is not held. The public or political perception that non-eligible people operating under fraudulent identities are receiving services from agencies leads to a loss of the agencies' credibility with the public.

— Other loss or liability

EXAMPLE 4 The service provider is in breach of legislation or policy; an individual is prevented from gaining medical treatment, undertaking training, accessing a facility etc.

The applicable consequences and the affected parties should be determined.

10.5 Risk impact assessment

The risk impact assessment methods can be found in Annex B, which contains information on assessing the degree of impact of a consequence, assigning a level to an assessed impact, control selection and effectiveness, assessing likelihood and plotting level of risk. For more methods, refer to ISO/IEC 27005.

11 Identity-related risk evaluation

In this assessment of identity-related risk, the level of risk is also used to indicate the ideal strength of the identity processes to be applied. Each risk drives a different identity process. For example:

— The strength of identity information accuracy is driven by the overall level of risk for incorrect information provided for a service or transaction.

— The strength of initial binding and ongoing authentication of an individual is driven by the overall level of risk for someone incorrectly linked to or associated with the information or authenticator used in a service or transaction.

Identity processes for registration of individuals and authentication of returning individuals varies in comprehensiveness depending on the level of identity-related risk contained in the particular transaction. In general, the greater the level of inherent identity-related risk for a transaction, the more comprehensive and stringent the identity process should be.

The identity processes and their strength become additional controls for identity-related risks. Applying the ideal identity process strength in conjunction with the identified controls should result in a net impact score close to 1.

Depending on the standards used by the organization for identity processes, the level of risk can be used to determine strengths on scales of either 3 or 4 strengths. Tables 2 and 3 provide the conversion of the level of risk into 3 and 4 strengths, respectively.

Table 2 — Converting level of risk into 3 strengths

Level of risk 1	Level of risk 2	Strength of identity process
1–10	1 - 6	Low – Level 1
11–19	7 - 19	Moderate – Level 2
20 - 25	20 - 25	High – Level 3

Table 3 — Converting level of risk into 4 strengths

Level of risk 1	Level of risk 2	Strength of identity process
1 - 3	1–3	Low – Level 1
4 - 6	4–10	Moderate – Level 2
7 - 19	11–19	High – Level 3
20 - 25	20–25	Very high – Level 4

NOTE Transactions described as having no risk do not require a strength value in either of the above tables.

While the identity-related risk assessment should be carried out for each transaction and each transaction, therefore having its own pair of identity process strengths, an organization may choose to roll transactions up into a single service. In this case, the highest strength value associated with each of the two risks or identity processes should be taken as the strength required for the service.

12 Identity-related risk treatment

Risk treatment is part of risk management. For more information on this matter, see ISO 31000.

Annex A
(informative)

Standards related to identity-management risk assessment

A.1 Standards related to risk management guidance

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

ISO 31000:2018 presents guidelines on risk management for organizations. In doing so, it defines risk assessment as the overall process of risk identification, risk analysis and risk evaluation, and places risk assessment as one part of the overarching approach to risk management. This document expands on these concepts with a specific focus on identity risk considerations.

A.1.2 Risk assessment techniques defined in IEC 31010:2019

IEC 31010:2019 provides guidance on the selection and application of techniques for assessing risk in a wide range of situations. The techniques are used to assist in making decisions where there is uncertainty and to provide information about particular risks; these techniques are applied as part of the process for managing risk. IEC 31010 provides summaries of a range of techniques, with references to other documents where the techniques are described in more detail. It provides guidance on the use, implementation and selecting of risk assessment techniques. For implementation, IEC 31010 provides planning, management, apply, review and record processes in detail. IEC 31010:2019 includes the following significant technical changes with respect to IEC 31010:2009[1)], in particular:

— more detail is given on the process of planning, implementing, verifying and validating the use of the techniques;

— the number and range of application of the techniques has been increased;

— the concepts covered in ISO 31000 are no longer repeated in this document.

A.2 Standards on identity management guidance

A.2.1 Identity management framework defined in ISO/IEC 24760

ISO/IEC 24760-1 defines terms for identity management and specifies core concepts of identity and identity management and their relationships.

ISO/IEC 24760-2 provides guidelines for implementing the system for managing identity information, and specifies requirements for the implementation and operation of a framework for identity management.

ISO/IEC 24760-3 is applicable to an identity management system where identifiers or personally identifiable information relating to entities are acquired, processed, stored, transferred or used for the purposes of identifying or authenticating entities, or for the purpose of decision making using attributes of entities.

ISO/IEC 24760-1, ISO/IEC 24760-2 and ISO/IEC 24760-3 discuss the need to carry out risk assessment (both identity-related and security) and mention the general steps to do so, but provide no further guidance.

1) Withdrawn.

A.2.2 Identity proofing defined in ISO/IEC TS 29003

ISO/IEC TS 29003 gives guidelines for the identity proofing of a person, and specifies levels of identity proofing and requirements to achieve these levels. The document is applicable to identity management systems.

A.2.3 Entity authentication described in ISO/IEC 29115

ISO/IEC 29115 provides a framework for managing entity authentication assurance in a given context. In particular, it:

— specifies four levels of entity authentication assurance;

— specifies criteria and guidelines for achieving each of the four levels of entity authentication assurance;

— provides guidance for mapping other authentication assurance schemes to the four levels of assurance (LoAs);

— provides guidance for exchanging the results of authentication that are based on the four LoAs;

— provides guidance concerning controls that should be used to mitigate authentication threats.

A.2.4 Authorization/access control described in ISO/IEC 29146

ISO/IEC 29146 defines and establishes a framework for access management (AM) and the secure management of the process to access information, and information and communications technologies (ICT) resources, associated with the accountability of a subject within some context.

ISO/IEC 29146 provides concepts, terms and definitions applicable to distributed access management techniques in network environments.

ISO/IEC 29146 also provides explanations about related architecture, components and management functions.

The subjects involved in access management can be uniquely recognized to access information systems, as defined in the ISO/IEC 24760 series.

The nature and qualities of physical access control involved in access management systems are outside the scope of ISO/IEC 29146.

A.2.5 Trust anchors for DLT-based identity management (TADIM) described in ISO/TR 23644

ISO/TR 23644 defines trust anchors for distributed ledger technology (DLT)-based identity management (under development).

Figure A.1 shows a summary of the standards relevant to identity-related risk assessment.

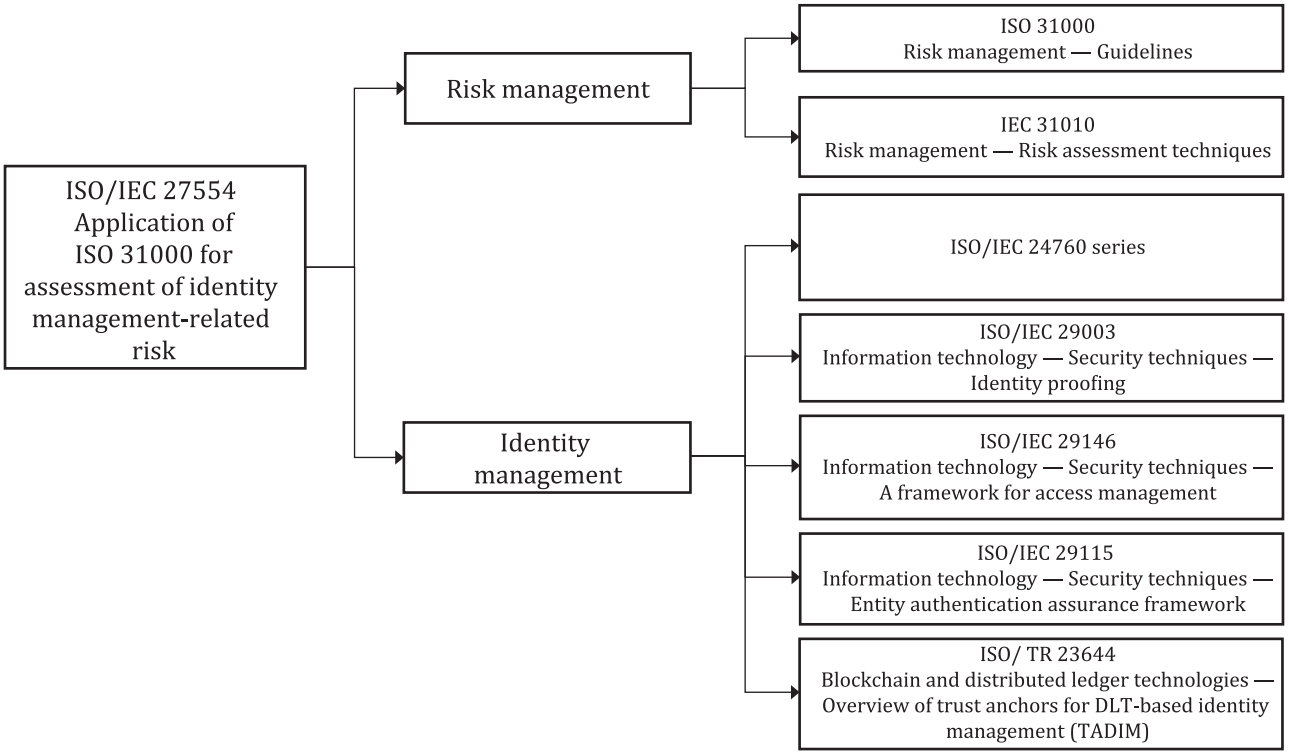

Figure A.1 — Standards for identity-related risk assessment

Annex B
(informative)

Risk impact assessment

B.1 Assessing the degree of impact of a consequence

Care should be taken to avoid cascading the impacts of consequences onto subsequent events, which can result in over-inflation of impact levels, especially if event risk moves beyond the initial risk source.

EXAMPLE 1 As the result of a transaction, a driving licence is issued to someone other than the entitled individual. A consequence of this transaction is that the incorrectly issued license can be used as identification to access a benefit at another organization. The direct impact of the subsequent use of that benefit does not fall on the organization issuing the identity-related document. Instead, there is potentially harm to the other organization, which placed trust in the validity of the document.

EXAMPLE 2 As the result of a transaction, sensitive information is accessed by an unauthorised party. Potential consequences of this transaction include:

a) The unauthorised party uses the information to blackmail the entitled individual or to find them and inflict bodily harm. These are identity-related consequences of this transaction.

b) The unauthorised party publishes the information causing distress to the entitled individual.

c) As a result of their employer, colleagues or customers becoming aware of the information, the entitled individual is terminated from their job. The loss of the job is not an immediate direct consequence of this transaction, but is a consequence of the third party's subsequent use of, and their employers reaction to the disclosed information.

For each risk and its consequences, the organization should identify:

— which parties will be impacted;

— how each party will be impacted (e.g. monetary amounts, type of information, regulatory compliance, nature of inconvenience, media coverage);

— the degree of impact, where feasible using a value on an appropriate scale.

An outcome is not considered a consequence of a transaction, for risk assessment purposes, if there is no impacted party or if the impact is considered to be negligible by all parties.

The potentially impacted parties in Example 1 include:

— the individual legitimately entitled to the mis-issued identity;

— public authorities who are unable to collect traffic fines or similar due to the use of the identity to mis-direct the blame for traffic offences;

— service providers who give service access to the un-entitled user of the mis-issued identity, thereby reducing their capacity;

— legitimate users of a service which has been defrauded, due to reduced capacity for those users.

B.2 Assigning levels to the assessed impact

Once the impact, on each affected party, of each consequence and each identity-related risk, has been assessed and documented, it can be assigned a level using the guidelines for assessing identity-related impact levels provided in B.3 as a reference method.

For each consequence with an assessed impact, the level structure used in the example in B.3 has five ordered and subjectively defined levels:

— 1 Minimal;

— 2 Minor;

— 3 Moderate;

— 4 Significant;

— 5 Severe.

The levels assigned to the assessed impact of each risk are combined, collapsing the distinct indicators into a single combined value, as an indicator of identity-related risk in B.4.

B.3 Impact level guide

Organizations use their own scales for determining the level of impact and likelihood of events with identity-related consequences. These scales normally align with wider risk assessment activities in the organization, be that at enterprise-level, in specific parts of the organization, or for crosscutting risk-relevant themes. Table B.1 provides an example of generic descriptions for degrees of impact and levels of identity-related consequences that can be adapted and adopted by an organization. The subjective terms, such as “minor”, should be defined by the organization in alignment with their cultural values and assumptions, consistently with other elements of their overarching risk management framework.

Table B.1 — Generic degree of impact descriptions

	Financial loss or liability	**Release/disclosure of information**	**Qualification/ reputation**	**Other loss or liability**
Impact on entitled individual				
1 Minimal	Some minor inconvenience (E.g. minimal amount, short-term, recoverable)	Some minor inconvenience (E.g. generally available from other sources, easily recoverable or revocable)	Some minor inconvenience	Some minor inconvenience
2 Minor	Inconvenience or minor distress (E.g. moderate amount or extended term delaying recovery)	Inconvenience or minor distress (E.g. some non-public information)	Inconvenience or minor distress	Inconvenience or minor distress
3 Moderate	Some hardship, significant inconvenience, moderate distress or short-term public embarrassment (E.g. moderate amount or extended term causing some hardship)	Minor injury, significant inconvenience, moderate distress or short-term public embarrassment (E.g. impacting character or location, causing undesirable or threatening attention)	Minor injury, significant inconvenience, moderate distress or short-term public embarrassment	Minor injury, significant inconvenience, moderate distress or short-term public embarrassment
4 Significant	Unrecoverable, significant distress or sustained public embarrassment (E.g. significant amount, long term loss causing sustained hardship)	Temporary injury, significant distress or sustained public embarrassment (E.g. impacting character or location, causing attention of a physical or sustained nature)	Temporary injury, significant distress or sustained public embarrassment	Temporary injury, significant distress or sustained public embarrassment

Table B.1 *(continued)*

	Financial loss or liability	**Release/disclosure of information**	**Qualification/ reputation**	**Other loss or liability**
5 Severe	Loss of personal liberty or bankruptcy	Loss of personal liberty, permanent injury or death	Loss of personal liberty, permanent injury or death	Loss of personal liberty, permanent injury or death
Impact on service provider				
1 Minimal	Some minor inconvenience	Some minor inconvenience	Some minor inconvenience	Some minor inconvenience
2 Minor	Noticeably reduced effectiveness of a primary function, minor damage to assets	Noticeably reduced effectiveness of a primary function, minor damage to assets	Noticeably reduced effectiveness of a primary function, minor damage to assets	Noticeably reduced effectiveness of a primary function, minor damage to assets
3 Moderate	Significantly reduced effectiveness of a primary function, moderate damage to assets, trust in service impacts usage	Significantly reduced effectiveness of a primary function, moderate damage to assets, trust in service impacts usage	Significantly reduced effectiveness of a primary function, moderate damage to assets, trust in service impacts usage	Significantly reduced effectiveness of a primary function, moderate damage to assets, trust in service impacts usage
4 Significant	Severe function degradation or inability to perform one or more functions, major damage to assets, loss of trust affecting wider organization	Severe function degradation or inability to perform one or more functions, major damage to assets, loss of trust affecting wider organization	Severe function degradation or inability to perform one or more functions, major damage to assets, loss of trust affecting wider organization	Severe function degradation or inability to perform one or more functions, major damage to assets, loss of trust affecting wider organization
5 Severe	Cessation of business	Cessation of business	Cessation of business	Cessation of business
Impact on wider community				
1 Minimal	Some minor inconvenience	Some minor inconvenience	Some minor inconvenience	Some minor inconvenience
2 Minor	Inconvenience or minor distress, reduced effectiveness of a function, minor damage to an asset or a minimal number of parties impacted	Inconvenience or minor distress, reduced effectiveness of a function, minor damage to an asset or a minimal number of parties impacted	Inconvenience or minor distress, reduced effectiveness of a function, minor damage to an asset or a minimal number of parties impacted	Inconvenience or minor distress, reduced effectiveness of a function, minor damage to an asset or a minimal number of parties impacted
3 Moderate	Some hardship, significant inconvenience, moderate distress or short-term embarrassment, significantly reduced effectiveness of a function, moderate damage to assets or a moderate number of parties impacted	Minor injury, significant inconvenience, moderate distress or short-term embarrassment, significantly reduced effectiveness of a function, moderate damage to assets or a moderate number of parties impacted	Minor injury, significant inconvenience, moderate distress or short-term embarrassment, significantly reduced effectiveness of a function, moderate damage to assets or a moderate number of parties impacted	Minor injury, significant inconvenience, moderate distress or short-term embarrassment, significantly reduced effectiveness of a function, moderate damage to assets or a moderate number of parties impacted
4 Significant	Unrecoverable, significant distress or sustained embarrassment, severe function degradation or inability to perform multiple functions, major damage to assets or a significant number of parties impacted	Temporary injury, significant distress or sustained embarrassment, severe function degradation or inability to perform multiple functions, major damage to assets or a significant number of parties impacted	Temporary injury, significant distress or sustained embarrassment, severe function degradation or inability to perform multiple functions, major damage to assets or a significant number of parties impacted	Temporary injury, significant distress or sustained embarrassment, severe function degradation or inability to perform multiple functions, major damage to assets or a significant number of parties impacted

Table B.1 *(continued)*

	Financial loss or liability	Release/disclosure of information	Qualification/ reputation	Other loss or liability
5 Severe	Loss of personal liberty or bankruptcy or cessation of any business	Loss of personal liberty, permanent injury or death or cessation of any business	Loss of personal liberty, permanent injury or death or cessation of any business	Loss of personal liberty, permanent injury or death or cessation of any business

B.4 Control selection and effectiveness

Controls can be divided into four types: preventative, corrective, detective and directive. Controls are only effective if they apply in all cases. If a control can only be applied to a portion of the transactions, the effectiveness of that control should be assessed separately – specifically in the context of the set of transactions to which it applies.

The level of identity required to register an individual for a service and the level of authentication for an individual returning to a service are not counted as controls at this point as the strength of these will be determined later in the process.

Table B.2 provides a description of each control type.

Table B.2 — Control types and description

Control types	Description
Preventative	Stops the consequence or its impact from happening
Corrective	Does not stop a consequence from occurring but reduce the degree of impact
Detective	Identifies events and other signals indicative of a consequence or impacts so that corrective measures can be undertaken [a]
Directive/disincentive	Rules, policies, training or a lack of value in the service that may contribute to a general reduction in likelihood.

[a] Relies on the corrective measure which is undertaken being effective.

For each risk and its consequences, the organization should establish:

— which controls are in place;

— the effectiveness of the applicable controls.

B.1 lists examples of identity-related risk controls.

B.5 Likelihood assessment

Once the existing controls have been identified and their effectiveness determined, the organization should assess the likelihood of an event happening that results in any of the identity-related risks being realized. The likelihood is conditional on the controls being in place.

The extent to which an organization can accurately establish likelihood will vary. However, the following can help:

— experience of other services conducted by the organization that have similar identity-related risk exposures;

— experience of other organizations services that have similar identity-related risk exposures;

— relevant published data on the likelihood of particular identity-related events occurring for particular service types;

— availability of specialist and expert advice.

Organizations should not assume that because an event has not yet occurred, that it will never occur. The following list describes five levels of likelihood:

— Rare – robust controls are in place that prevent an event from occurring in all but the most exceptional circumstances;

— Unlikely – many controls are in place with some minor ineffectiveness that can allow an event to happen in limited circumstances;

— Possible – several controls are in place with such ineffectiveness that an event should occur in some circumstances;

— Likely – minimal controls are in place or controls lack effectiveness, such that it is highly probable an event will happen;

— Almost certain – there are no effective controls in place to prevent an event from happening.

For each risk and its consequences, the organization should estimate the likelihood of an event occurring given their assessment of the overall application.

B.6 Plotting level of risk

For each identified risk, the organization should plot each of the consequence impact and likelihood score combinations on a table, an example of which is shown in Table B.3.

Table B.3 — Plot matrix for level of risk

Likelihood	Level of assessed impact				
	Minimal	Minor	Moderate	Significant	Severe
Rare	1	2	4	7	11
Unlikely	3	5	8	12	16
Possible	6	9	13	17	20
Likely	10	14	18	21	23
Almost certain	15	19	22	24	25

Generally, the highest number achieved by any combination of the level of assessed impact and likelihood for each risk will indicate the two levels of risk for the transaction.

While applying the appropriate controls to a transaction is an important aspect of the management of identity-related risk, the remaining level of risk can be offset by applying the appropriate strength of the identity processes.

Bibliography

[1] ISO 9000:2015, *Quality management systems — Fundamentals and vocabulary*

[2] ISO/TR 23644, *Blockchain and distributed ledger technologies (DLTs) — Overview of trust anchors for DLT-based identity management*

[3] ISO/IEC 24760-1:2019, *IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts*

[4] ISO/IEC 24760-2:2015, *Information technology — Security techniques — A framework for identity management — Part 2: Reference architecture and requirements*

[5] ISO/IEC 24760-3:2016, *Information technology — Security techniques — A framework for identity management — Part 3: Practice*

[6] ISO/IEC 27005, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*

[7] ISO 28002:2011, *Security management systems for the supply chain — Development of resilience in the supply chain — Requirements with guidance for use*

[8] ISO/IEC TS 29003:2018, *Information technology — Security techniques — Identity proofing*

[9] ISO/IEC 29115:2013, *Information technology — Security techniques — Entity authentication assurance framework*

[10] ISO/IEC 29134:2023, *Information technology — Security techniques — Guidelines for privacy impact assessment*

[11] IEC 31010:2019, *Risk management — Risk assessment techniques*

[12] ISO 31073:2022, *Risk management — Vocabulary*

[13] *New Zealand Identity-related Risk Assessment Guidelines*

ICS 35.030; 03.100.01
Price based on 18 pages