

ISO/TC 262

Secretariat: BSI

Voting begins on:
2023-05-22

Voting terminates on:
2023-07-17

Risk management — Guidelines for managing emerging risk to enhance resilience

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/DTS 31050

<https://standards.iteh.ai/catalog/standards/sist/f5b301e8-ccd3-4aba-afdb-99ff0596925b/iso-dts-31050>

Member bodies are requested to consult relevant national interests in ISO/TC 292 before casting their ballot to the e-Balloting application.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.



Reference number
ISO/DTS 31050:2023(E)

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/DTS 31050

<https://standards.iteh.ai/catalog/standards/sist/f5b301e8-ccd3-4aba-afdb-99ff0596925b/iso-dts-31050>



COPYRIGHT PROTECTED DOCUMENT

© ISO 2023

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	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Emerging risks	2
4.1 The nature of emerging risks.....	2
4.2 Characterization of emerging risks.....	3
4.2.1 General.....	3
4.2.2 Knowledge aspects.....	4
4.2.3 Measurement aspects.....	5
4.2.4 Time dimension.....	5
4.2.5 Volatility aspects.....	6
4.3 Development of emerging risks.....	6
4.4 Relationship between managing emerging risks and organizational resilience.....	6
5 Principles	7
5.1 General.....	7
5.2 Integrated.....	8
5.3 Structured and comprehensive.....	8
5.4 Customized.....	8
5.5 Inclusive.....	8
5.6 Dynamic.....	8
5.7 Best available information.....	8
5.8 Human and cultural factors.....	9
5.9 Continual improvement.....	9
6 Process	9
6.1 Applying the ISO 31000 process to emerging risks.....	9
6.2 Communication and consultation.....	9
6.3 Scope, context and criteria.....	10
6.3.1 Scope and context.....	10
6.3.2 Criteria.....	11
6.4 Risk assessment.....	12
6.4.1 General.....	12
6.4.2 Identifying emerging risks.....	12
6.4.3 Analysing emerging risks.....	13
6.4.4 Evaluating emerging risks.....	15
6.5 Risk treatment.....	15
6.6 Monitoring and review.....	16
6.7 Recording and reporting.....	16
7 Enhancing resilience by managing emerging risks	17
7.1 Capability development.....	17
7.2 Emerging risks and resilience indicators.....	18
8 Risk intelligence cycle and managing emerging risks	20
8.1 Overview.....	20
8.2 Applying knowledge to decisions on emerging risks.....	21
Annex A (informative) Examples of changes in context that can be sources of emerging risks	23
Annex B (informative) Example of emerging risks description or recording template	24
Annex C (informative) Systemic risks	26

Annex D (informative) Example factors that can influence managing emerging risks	27
Annex E (informative) Knowledge and the risk intelligence cycle for managing emerging risks	29
Annex F (informative) Example of a completed resilience indicator template	33
Bibliography	35

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/DTS 31050](https://standards.iteh.ai/catalog/standards/sist/f5b301e8-ccd3-4aba-afdb-99ff0596925b/iso-dts-31050)

<https://standards.iteh.ai/catalog/standards/sist/f5b301e8-ccd3-4aba-afdb-99ff0596925b/iso-dts-31050>

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes 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 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. ISO 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.

This document was prepared by Technical Committee ISO/TC 262, *Risk management*, in collaboration with Technical Committee ISO/TC 292, *Security and resilience*.

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.

Introduction

Emerging risks are characterized by their newness, insufficient data, and a lack of verifiable information and knowledge needed for decision-making related to them. As these risks can develop with the potential for large threats and opportunities, appropriate management of emerging risks should be established as a part of an organization's risk management. It should include changes in circumstances or conditions related to multiple aspects of the organization's external context and the implications for its internal context.

Emerging risks can include, for example:

- risks arising from unrecognized changes in organizational contexts;
- risks created by innovation or social and technological development;
- risks related to new sources or previously unrecognized sources of risk;
- risks from new or modified processes, products or services.

Consequences of emerging risks can include, for example:

- exposure to unforeseen hazards and threats with uncertain outcomes;
- increased exposure to hazards and threats from known risk sources;
- lost or gained opportunities.

Managing emerging risk should be knowledge-focused and dependent on the need to accumulate verifiable data and information, especially when these are limited or inconsistent. With interpretation, this information forms knowledge and creates intelligence for strategic, tactical and operational decision-making.

ISO/DTS 31050

To this aim, this document provides guidelines for applying ISO 31000 to managing emerging risks to enhance organizational resilience. The focus is on emerging risks potentially having the most significant consequences for the organization and its objectives. Applying the ISO 31000 principles and process to managing emerging risk requires an understanding of the different aspects of the context in which the organization operates. In particular, this applies to the following:

- the continual scanning of changing circumstances or conditions that can result in an emerging risk helps to develop knowledge and provide the intelligence needed for strategic, tactical and operational decision-making;
- the identification of changes in an organizational context are often early indicators or signals that identify vulnerabilities and the sources of emerging risks;
- managing emerging risks relies on the application of the ISO 31000 principles under conditions of extreme uncertainty, increasing volatility, complexity and ambiguity within the multiple aspects of the context in which the organization operates.

Specific guidance is provided on:

- how to understand the nature and characteristics of emerging risks (see [Clause 4](#));
- how the principles of risk management apply to emerging risks (see [Clause 5](#));
- how the ISO 31000 risk management process is applied to emerging risks (see [Clause 6](#));
- how resilience can be enhanced by managing emerging risks (see [Clause 7](#));
- how to use the risk intelligence cycle for emerging risks (see [Clause 8](#)).

Further details are provided in [Annexes A to F](#).

The application of this document helps organizations to benefit from:

- increased awareness, reducing the likelihood of failing to anticipate emerging risks;
- early recognition of emerging risks and increased level of preparedness and resilience;
- timely dissemination of data and exchange of information among stakeholders;
- alignment of actions on emerging risks across all aspects of organizational contexts.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/DTS 31050](https://standards.iteh.ai/catalog/standards/sist/f5b301e8-ccd3-4aba-afdb-99ff0596925b/iso-dts-31050)

<https://standards.iteh.ai/catalog/standards/sist/f5b301e8-ccd3-4aba-afdb-99ff0596925b/iso-dts-31050>

Risk management — Guidelines for managing emerging risk to enhance resilience

1 Scope

This document gives guidance on managing emerging risks that an organization can face. It complements ISO 31000.

This document is applicable to any organization, at any stage and to any activity of the organization. Its application can be customized to suit different organizations or the context of different 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 22300, *Security and resilience — Vocabulary*

ISO 22316, *Security and resilience — Organizational resilience — Principles and attributes*

ISO 31000, *Risk management — Guidelines*

IEC 31010, *Risk management — Risk assessment techniques*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22300, ISO 22316, ISO 31000, IEC 31010 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

resilience attribute

feature or characteristic of an organization's ability to absorb and adapt to a changing context

3.2

knowledge

outcome of the assimilation of information through learning

Note 1 to entry: Knowledge can be acquired through research, experience or education.

Note 2 to entry: Knowledge includes information, facts, principles, theories and practices related to a field of work or study.

Note 3 to entry: Knowledge can be individual or collective. Collective knowledge is gained from people collaborating and releasing their tacit and subconscious knowledge.

[SOURCE: ISO 56000:2020, 3.4.1]

3.3 intelligence

result of gathering, analysing and interpreting data, information and *knowledge* (3.2)

Note 1 to entry: Intelligence can be of different kinds, e.g. (but not limited to) market, technology, competition, intellectual property or business.

[SOURCE: ISO 56006:2021, 3.1]

3.4 organizational resilience

ability of an organization to absorb, recover and adapt in a changing context

[SOURCE: ISO 22300:2021, 3.1.167, modified — “recover” added.]

3.5 radical innovation breakthrough innovation

innovation with a high degree of change

Note 1 to entry: Change can relate to the entity or its impact.

Note 2 to entry: Radical innovation is at the other end of the continuum to incremental innovation.

[SOURCE: ISO 56000:2020, 3.1.1.1]

3.6 disruptive innovation

innovation initially addressing less demanding needs, displacing established offerings

Note 1 to entry: Compared to established offerings, disruptive innovations are initially simpler offerings with lower performance and they are generally more cost effective, requiring fewer resources and offered at lower cost.

Note 2 to entry: Disruption occurs when a significant ratio of users or customers have adopted the innovation.

Note 3 to entry: Disruptive innovations can create new markets and value networks by addressing new users and deploying new business and value realization models.

[SOURCE: ISO 56000:2020, 3.1.1.2]

4 Emerging risks

4.1 The nature of emerging risks

The nature of emerging risks (see the examples in [Annex A](#) and the example of data to be collected about them in [Annex B](#)) can include:

- risks that have not been previously recognized or experienced by an organization;
- familiar risks in a new or unfamiliar context where the existing knowledge is not applicable;
- significantly evolving risk;
- systemic risks (see [Annex C](#));
- a novel combination of risks.

If an organization does not consider emerging risks, it does not mean that the organization will not be affected. In many cases, it is initially not possible to formulate scenarios of interest in, to estimate event likelihood, to anticipate consequences or to identify control options. To better understand the

nature of the particular emerging risk, the nature of similar risks that are better understood should be considered.

The above risks can stem from changes of context in which the organization seeks to meet its objectives, such as:

- organizational relationships;
- access to capital and capabilities;
- interactions or interdependencies with societal, geopolitical, environmental, economic, technological, legal, perception (see [Annex D](#)) and ethical factors;
- the internal governance, cultural and operational aspects of its business.

Emerging risks should be proactively identified and characterized from observing changes in organizational contexts. Emerging risks are typically represented by a set of new circumstances or conditions, not previously recognized, or changes in the characteristics of already identified risks. The changes can be related to, for example:

- societal norms;
- organizational culture;
- perceptions;
- data, or information interpreted from data, about a risk or the way that risk evolves.

NOTE There are occasions when risks emerge with little prior visibility in the context.

4.2 Characterization of emerging risks

4.2.1 General

Effective and efficient management of emerging risk requires the continual acquisition of knowledge about the organization's function, context, experience, access to data and emerging risk characteristics (e.g. by applying the risk intelligence cycle, see [Clause 8](#) and [Annex E](#)). The data, information and knowledge acquired should be recorded appropriately (see [6.7](#) and [Annex B](#)).

The following factors can be of particular importance for the new knowledge about emerging risks:

- a) possible deviations from the expected outcomes or consequences, either positive or negative, and their likelihood;
- b) sources and nature of risks;
- c) other factors, such as the rate of development of risk and detectability.

Where the organization has not previously experienced particular changes in its context, it is possible that data related to those changes are limited or that all characteristics of emerging risks are not evident (e.g. for systemic risks, see [Annex C](#)). Understanding the characteristics of emerging risks context depends upon available knowledge relating to nature and source, quantity and time, in a volatile, uncertain context, complex and ambiguous circumstances. Consequently, the knowledge acquired can be insufficient to identify changes in characteristics and potential sources of risk or, if an emerging issue has been identified, to determine the likelihood and consequences of deviations from expectations.

Due to high uncertainty, the interpretation of data and information can be biased by individual perceptions (see [Annex D](#)).

Emerging risk characteristics should be categorized, for example, by considering the following elements:

- knowledge elements, including, for example:
 - unknown changes in organizational contexts;
 - weak signals of change subject to interpretation and bias;
 - insufficient data to determine likelihood and consequences;
- volatility elements, including, for example:
 - conditions or circumstances likely to change, rapidly or unpredictably;
 - impact of change and consequences of an unknown variable;
 - instability of data and information;
- uncertainty elements, including, for example:
 - transition from early warnings and signals to emerging risks;
 - determination of sources of emerging risks;
- complexity elements, including, for example:
 - high level of interconnectedness of systems, parts or processes;
 - unknown interdependencies throughout the organization's context;
 - interactions of emerging risks with other risks or activities that can result in non-linear effects;
 - the systemic nature of certain risks (see [Annex C](#));
 - large degree of complexity of potential decisions and consequences;
- ambiguity elements, including, for example:
 - limited data open to multiple interpretations and individual perceptions;
 - lack of precedence for the development of knowledge and intelligence;
 - lack of clarity on the cause and effect of changes in contexts;
- time dimension elements, including, for example:
 - velocity of change in the organization's context;
 - rate of change in characteristics of emerging risks;
- controllability elements, including, for example, the effects of factors out of the organization's control, both in internal and external contexts;
- behavioural elements, including, for example, the effects of unexpected changes in contexts, people, systems or processes (see [Annex D](#)).

Not all of the above characteristics apply necessarily to all emerging risks and are not unique to emerging risks. The above categories, however, do represent a common theme for emerging risks, which should be considered when managing them.

4.2.2 Knowledge aspects

Knowledge relating to emerging risks should be based on the quantity and quality of data available and their usability as credible information to support decision-making. In order to manage emerging

risks effectively, the use of systems that can gather and interpret data about capabilities, possibilities, changes and trends in the external context should be considered, taking into account that the knowledge about emerging risk characteristics and their influence on the organization's objectives can depend on the data still missing or that are limited.

It should be noted that in the absence of adequate knowledge, understanding of emerging risks can be influenced by individual perceptions, cognitive bias, group dynamics, misinformation or misinterpretation, preventing the reliable assessment of likelihoods and consequences. In such cases, the focus of managing emerging risks should be on assessing their plausibility^[4] and enhancing the organization's resilience^[5].

As emerging risks evolve, knowledge about them and their characteristics also evolves with time.

NOTE Initially, there can be little understanding of the potential for issues arising from particular circumstances. As data and information are collected and interpreted, knowledge increases, enabling organizations to identify emerging risks and make decisions about their potential consequences.

This should be defined within the risk intelligence cycle. The application of knowledge as strategic intelligence and improved decision-making should be systematic. See [Clause 8](#) and [Annex E](#).

4.2.3 Measurement aspects

The quality (e.g. integrity, reliability, accuracy, timely, relevancy) of available data and information is essential for acquiring the knowledge necessary to assign values to the measurable elements of emerging risk characteristics, including consequences and likelihood. The organization should establish a system for timely acquisition of relevant data on weak signals or early warnings, as well their analysis and analysis of changes in emerging risk characteristics. This analysis should include the ambiguity of information, its limitations related to understanding the development of emerging risks, and trends and patterns in the organization's context, indicating the source of possible emerging risks.

4.2.4 Time dimension

Characterizing emerging risks should include the time dimensions, such as the rate at which information necessary to understand and manage risk becomes available. Understanding the time-related characteristics of emerging risks also influences data collection and analysis, the interpretation of information and the creation of knowledge for timely decision-making in managing emerging risks.

Time until the necessary information becomes available also affects risk management control options and the extent of expertise required.

Key time indicators as characteristics of emerging risks should include:

- a) the rate (velocity) of change in conditions or circumstances;
- b) the rate of development of an emerging risk;
- c) the lead time from a change in circumstances or conditions to the identification of an emerging risk;
- d) the time to reach the maturity of data essential to information, knowledge and intelligence;
- e) the time between context changes and the appearance of weak signals or early warnings;
- f) the time from risk identification to event occurrence.