TECHNICAL SPECIFICATION

ISO/TS 31050

First edition
2023-10

Risk management — Guidelines for managing an emerging risk to enhance resilience

Management du risque — Lignes directrices relatives à la gestion des risques émergents afin d'améliorer la résilience

Reference number
ISO/TS 31050:2023(E)

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) 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 the 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.

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 the 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 is often an early indicator or signal that identifies 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.

Risk management — Guidelines for managing an emerging risk to enhance resilience

1 Scope

This document gives guidance on managing emerging risks that an organization can face. This document 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” has been added and "environment" has been replaced with "context" in the definition.]

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 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, 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 the 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.

4.2.5 Volatility aspects

The emerging risk characteristics potentially leading to uncertain or unexpected changes and volatility in the emerging risk can include:

— sudden recognition that circumstances are not understood well enough and that the organization is unaware of potentially important data;

— unexpected and unanticipated step changes in contexts, capabilities and understanding of the implications of those changes;

— rapid and unpredictable variability and unforeseen changes in the organizational context.

Information should be continually updated to increase the understanding of the reasons for these changes. The characteristics and knowledge should be included as part of effective and efficient decision-making on emerging risks.

4.3 Development of emerging risks

Understanding the various aspects of the organizational context should be considered as the key to effective identification, analysis and evaluation of the emerging risk (see 4.1). Changes in any or all these environmental aspects create changes in the organizational context with the potential to impact organizational objectives, either positively or negatively.

Weak signals and first indicators of change in any aspect of the organization's context are precursors to potential emerging risk. In these circumstances, organizations should monitor identified changes in any aspect of their context and continually gather and analyse data to determine the significance of a change in any element or aspect, and to develop scenarios.

Close monitoring and review of changes in contexts, and increasing availability of data such as likelihood, rate of change, magnitude and volatility of occurrence, time horizons and aspects of the organization's context, all contribute to clarity and a better understanding of identified issues and potential emerging risks.

During the initial stages of an emerging risk development, the organization, especially one having little or no previous knowledge or experience with emerging risks, should be aware that data can be unavailable, limited, inconsistent, inaccurate or false. The process of interpretation of data into verifiable information for decision-making should be, therefore, focused on reducing significant uncertainties.

Although the continual monitoring and review of changes in characteristics of an emerging risk will generally increase the quality and quantity of data collected, the organization should be aware of circumstances where not all changes in its context can be identified or covered by the scenario analysis.

4.4 Relationship between managing emerging risks and organizational resilience

Organizational resilience enables an organization to deliver its objectives, survive and prosper. The changes in the organizational context are often early indicators or are those that identify threats and opportunities, vulnerabilities and the sources of an emerging risk.

With respect to possible threats, organizational resilience allows organizations to prepare for them, absorb their impacts, recover from them and adapt to the changing conditions. With respect to possible opportunities, organizational resilience allows organizations to adapt to gain from change, create internal value and take measured risks confidently (see ISO 22316).

Efficient and effective managing of emerging risks should help to preclude and mitigate possible failures to exploit opportunities or experience adverse effects on the organization's important objectives, or even the organization's survival.

Therefore, the organizations should adopt and apply the principles of resilience and resilience indicators (see Annex F). They should develop capabilities and attributes that enhance their ability to

survive and prosper. An organization's ability to anticipate, prepare and respond to change should be the key requirement for effectively managing emerging risks. Resilient organizations should, thus, be characterized by their abilities that include the following:

— Anticipation: The ability to prepare for unexpected or unlikely events by developing foresight capabilities and functions that are necessary to deal with any kind of unexpected event, both favourable and adverse. This also means being ready to take advantage of potential opportunities offered by changes in external contexts before competitors.

— Resistance and recovery: The ability to resist adverse situations and recover after disturbances and return to a normal state beyond the maintenance and restoration of organizational functionality, focusing on the advancement of organizational processes and capabilities.

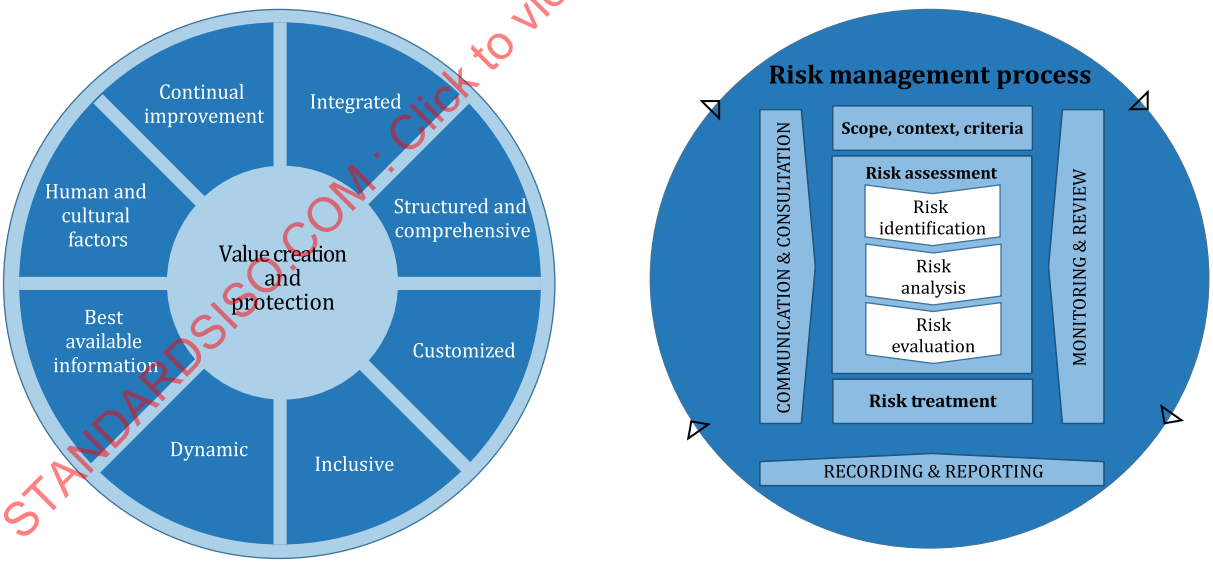
— Adaptation: The ability to effectively develop situation-specific responses, adapt to disruptive events and ultimately engage in transformative activities to capitalize on disruptive events.

Determining an organization's level of resilience prior to a disruptive event should be measured and dependent upon the extent to which an organization has successfully managed a similar unexpected event. Organizational resilience should include capability through which effective anticipation and adaptation to emerging risks can be achieved.

5 Principles

5.1 General

The core of risk management and its purpose is value creation and protection. To achieve this, ISO 31000 outlines a set of principles, see Figure 1 a). These principles are equally applicable to the managing of emerging risk.



a) Principles **b) Process**

Figure 1 — Principles and process in ISO 31000

Subclauses 5.2 to 5.9 give additional recommendations for applying those principles to managing emerging risk. When applying these principles, the organization should ensure that emerging risks:

— are reviewed continually during their emerging stages to improve knowledge and understanding of their characteristics and state;

— are assessed considering a broad range of possible future situations.

In addition, the organization should ensure that threats and opportunities are adequately managed, recognizing the limitations, inconsistency, and variability of information and data.

5.2 Integrated

There is no additional guidance in addition to that provided in ISO 31000.

5.3 Structured and comprehensive

The organization should apply an agile approach where necessary for collecting and interpreting data, producing information and converting knowledge into intelligence for use by decision-makers (see Clause 8 and Annex E).

The organization should explicitly consider whether the acquisition of data (both structured and unstructured) and their interpretation as information and the knowledge applied satisfies the requirement of a comprehensive approach to risk management.

The approach should emphasize the importance of consistent identification, work and communication about emerging risks.

5.4 Customized

The organization should ensure its risk management framework and process are customized to reflect the volatility, uncertainty, complexity and ambiguity of emerging risks consistent with its mission, objectives and strategies.

5.5 Inclusive

The organization should identify and engage relevant stakeholders with an interest in the emerging risk in an appropriate and timely manner to improve the extent of the organization's knowledge by learning from the experiences of different stakeholders that the organization can apply.

Even when data quality is poor and information is limited, the organization should continue to recognize the credibility of the information if the source has sufficient credibility and expertise.

5.6 Dynamic

The organization should consider the potential for unexpected and disruptive changes in context. It should develop a timely capability to anticipate, detect and respond to change. The organization should, therefore, remain sufficiently agile, flexible and adaptable to accommodate plausible changes in the external context.

The organization should ensure its risk management framework includes components designed to anticipate and respond to changing circumstances and that sufficient flexibility exists within the risk management process. The members of the organization should be able to adapt and apply different tools and techniques to address the characteristics of emerging risks.

5.7 Best available information

Recognizing the lack of history and relevant current information when assessing emerging risks, the organization should ensure the ongoing development of data gathering and verification and data analysis to extract information relating to emerging risks to source the best information for decision-making.

Clause 8 provides additional guidance on how to gather all available data and produce valuable intelligence for decision-making regarding emerging risks.

5.8 Human and cultural factors

The organization should recognize that the lack of facts related to emerging risks can invalidate established views. For this reason, information on emerging risks can significantly impact human culture and behaviour. Therefore, the contribution of internal and external experts should be valued.

The organization should recognize that the availability and interpretation of data into credible information can change significantly as emerging risks develop. Early perceptions can prove incorrect, and previously established beliefs can be challenged.

5.9 Continual improvement

The organization should ensure that emerging risk management leads to new opportunities for society and business, new learning and new experiences, including a critical review of the results of previous risk analyses. The organization should explicitly identify this new level of understanding as a catalyst for knowledge development, new and improved processes, and practices in and beyond risk management.

The organization should ensure continual improvement leads to effective and efficient management of emerging risks. These improvements should include data collation, information transformation and sharing, and knowledge creation and enhancement while applying the risk management process.

Effective management of the emerging risk calls for foresight, which is also required for effective market intelligence work, and new product and service development in both the public and private sectors. Management of the emerging risk is fundamental to success in developing objectives and delivering service to meet current requirements while preparing for the future.

6 Process

6.1 Applying the ISO 31000 process to emerging risks

The organization should apply the risk management process described in ISO 31000:2018, Clause 6 [see Figure 1 b)] to manage emerging risks. It should integrate activities into its structure, system, operations and processes. The relevance of emerging risks should be considered at all levels and within each organization's function.

The application of the ISO 31000 process to emerging risks should use a structured approach with sufficient flexibility to adapt to the latest information as emerging risk understanding grows. For example, knowledge gained from risk analysis can be applied to anticipate changes in context.

Emerging risks can influence each other and other risks faced by the organization. The organization should consider emerging risks as part of a broader system rather than as discrete and individual issues by considering possible interdependencies and interconnectedness. An approach which analyses dependencies, relationships and interconnection should yield a thorough understanding beyond just examining the individual risk components without a view of the whole system.

The risk intelligence cycle described in Clause 8 and Annex E can assist organizations and their decision-makers in applying the risk management process described in ISO 31000.

6.2 Communication and consultation

In addition to ISO 31000:2018, 6.2, the following recommendations apply.

The organization should identify internal and external stakeholders and establish communication paths so that when action is needed, the means of communication are already established. As with any risk, stakeholders should include those who should be kept informed, those who will be consulted and those who will participate in the different elements of the risk management process. Stakeholders can change over time, and different stakeholders can be across different risk management elements. For example,

a wide range of unique experience and expertise can help identify emerging risks, while analysis of a particular risk can require specific subject matter experts.

Engaging with relevant stakeholders assists in the identification of emerging risks and enables stakeholders to provide information to support decisions and provide feedback on their implementation. It enables information and knowledge about emerging risks to be shared with and among different stakeholders (e.g. experts, regulators, shareholders, consumers, media, partners, suppliers, public services, the general public). In this way, they can reach a common understanding of the risks and the reasons behind any actions required to manage them.

There can be little knowledge of the implications of an emerging risk when it is first identified, and it is, therefore, likely that different perspectives and perceptions appear about its significance to the organization. Communication is essential for dealing with the different perceptions which can arise (e.g. from the influence of social media or the presentation of false or misleading information in media sources).

Rapidly developing emerging risks can necessitate swift decision-making, reinforcing the need for enhanced communication and consultation. The possibility that other organizations or stakeholders (e.g. partners, customers, suppliers) have experienced similar situations should be considered in order to try to obtain relevant data and information.

The organization should:

— establish an effective means of gathering up-to-date information about emerging risks and communicating it to help counteract misinformation;

— rapidly communicate changes in context and emerging risks that are identified in any instance of the risk management process throughout the organization;

— develop the capability to reach stakeholders quickly to ensure two-way communication (e.g. to provide critical information about emerging risks, get feedback, and enable the organization to adapt and respond to changing circumstances);

— establish a means by which those assessing emerging risks can influence the appropriate levels of authority so that plans can be enacted if and when the emerging risks reach certain thresholds;

— develop trust among relevant stakeholders (this is especially challenging when critical information is uncertain or ambiguous or there is no risk treatment option available);

— encourage and empower relevant stakeholders, whatever their position or status, to alert relevant people to issues where they perceive there can be an emerging risk.

6.3 Scope, context and criteria

6.3.1 Scope and context

In addition to ISO 31000:2018, 6.3, the following recommendations apply.

Organizations should consider multiple aspects of the context in which the organization exists. Sources of risk can arise from the organization's relationships, interactions or interdependencies with societal, geopolitical, environmental, economic, technological, legal and ethical factors, and the internal governance, cultural and operational aspects of its business. A broad view of the context and time horizon should be taken as sources of risk; weak signals and early warning signs of change can appear outside the immediate context. The breadth and depth of contextual information is critical to effectively managing emerging risks.

In addition to understanding the current context in which the organization operates, the organization should look for changes and trends that can be a source of emerging risks. Changes in context can be either internally driven (e.g. expanding into new areas) or externally driven (e.g. new technology). They can influence the organization directly or indirectly through affiliated organizations and sectors.

Changes can be gradual (e.g. climate change, a step change, a natural disaster) or rapid (e.g. a pandemic). In some cases, the potential for a context change can already be identified as a risk.

The significance of any changes in context should be assessed at the operational and strategic levels, as changes can have significant strategic and operational consequences.

When considering the context of emerging risk, the following recommendations apply.

— The scope of activities relating to emerging risks should have sufficient breadth to cover any changes that can give rise to risks to the organization's objectives. This can include political, economic, sociological, technological, legal and environmental changes, and changes in the human resources of the organization.

— The boundaries of the organization, systems, process, projects or activities for which risks will be assessed should be defined.

— The external factors that can influence (positively or negatively) the organization's ability to achieve its objectives and the ways that they can change should be identified and understood.

— The aspects of the internal context of an organization that can increase sensitivities and vulnerabilities to emerging risks should be understood.

— Mechanisms to monitor for changes in the internal and external context, including trends and changes that can occur gradually, should be established.

— Scenarios to provide an understanding of possible future states should be developed and analysed.

— Changes in how the organization's context develops should be continuously monitored (not only the changes themselves, but also how they are perceived in the organization's context, which can be a source of an emerging risk).

— resilience and its indicators when relevant emerging risks are detected should be evaluated (see Clause 7).

Periodic reviews of the internal and external context should be supplemented by continually scanning for changes. This enables data to be updated to improve understanding of the emerging risk and provides appropriate intelligence for their ongoing management (see also Clause 8 and Annex E).

Diverse information sources should be used to help provide an understanding of the context of emerging risks. This can include, for example, scanning the web, contacts with industry associations and other professional bodies, and informal professional networks.

NOTE The use of mnemonics such as PESTLE (political, economic, social, technological, legal, environmental) or STEEPLE (social, technological, economic, environmental, political, legal, ethical) can help provide a structured approach that directs attention to different areas of the context to consider.

6.3.2 Criteria

The organization should establish criteria and simple rules for deciding the significance of an emerging risk. However, in the case of emerging risk, there is often insufficient data and too much complexity or ambiguity to apply simple rules to decide significance. A decision about whether an emerging risk needs action is likely to be consultative and will take into account available evidence on different aspects, such as:

— degree of belief and justification as to whether a particular consequence can occur (plausibility);

— the nature of consequences and the magnitude of their possible effect on objectives;

— the perceived likelihood of occurrence of a particular scenario;

NOTE Likelihood of occurrence, plausibility and uncertainty in the magnitude of consequences are distinctive characteristics and thus, they are not interchangeable terms.

— the level of uncertainty in estimates of consequence and likelihood of occurrence;

— the speed with which changes are occurring;

— the time scale within which consequences can occur;

— the practicality of controls;

— relevant stakeholder's opinion.

For emerging risks, cause-and-effect relationships are not always fully established. The organization can, therefore, advise a precautionary and transparency-based approach (see Reference [6]) to decisions involving risk, particularly when an activity can potentially harm human health or the environment.

6.4 Risk assessment

6.4.1 General

In addition to ISO 31000:2018, 6.4, the recommendations given in 6.4.2 to 6.4.4 apply.

6.4.2 Identifying emerging risks

Initially, it is likely that the organization does not have previous knowledge and experience with emerging risks which are difficult to recognize and describe.

Changes in the context create and shape the development of emerging risks. Sources of emerging risks can include, for example, global attitude changes, innovative technologies, the actions of other organizations, political and economic pressures, and environmental and social change.

There can be positive and negative consequences for multiple objectives and cascading and compounding effects, and these are often not immediately obvious. Therefore, particular attention should be paid to using multiple methods/techniques and information sources for identifying the range of positive and negative consequences that can arise from one source of risk.

A structured approach to identifying emerging risks helps to ensure nothing obvious is missed, but some unstructured identification and data-gathering techniques are helpful to allow and encourage imaginative thinking. The use of multiple complementary methods and techniques can enable more comprehensive identification.

The organization should:

— undertake regular and comprehensive scanning of the context in which it operates from multiple perspectives or the use of relevant methods/techniques to identify changes in context and emerging risks;

— seek to identify emerging risks at a strategic level and throughout the organization whenever the risk management process is applied (risks of particular significance to individual projects or departments can be less visible or less likely to be considered during higher-level strategic thinking);

— analyse trends that can eventually lead to new risks;

— describe sources of risks and possible scenarios of interest associated with the above;

— actively seek scenarios with positive as well as negative outcomes;

— explore interconnected risks and contexts;

— identify indicators for emerging risks that will provide an early warning of imminent consequences or new opportunities and threats that are emerging and monitor these indicators;

— continually monitor data so that descriptions of risks can be updated as the latest information is obtained.

The IEC 31010 methods used for identifying and analysing risks can also be applied to emerging risks. Scenario techniques are beneficial for identifying consequences, cascading and compounding effects previously not encountered. Scenario analysis involves identifying multiple possible scenarios that can develop depending on the context and planning responses that lead to preferred future states.

Techniques that make people think from different perspectives are also helpful.

6.4.3 Analysing emerging risks

Risk analysis should aim to understand risk so that informed decisions can be made. Understanding should be ensured for decisions about:

— whether the emerging risk is significant for the organization (see 6.3.2);

— how the organization should respond to the emerging risk and with what urgency;

— selecting available options for planned actions.

The organization should pay special attention to emerging risks where the initial data are limited, knowledge about the risk is burdened by significant uncertainty (e.g. about possible scenarios, consequences or the effectiveness of controls), or interpreting such data as information for decision-making is affected by cognitive biases (see Annex D). In such cases, the organization should gather the best available data and information using reputable sources. Data and information should be verified where possible.

Given the characteristics of emerging risks, the organization should analyse sources of emerging risk, possible events and scenarios, and their positive and negative effects on objectives. The possibility of cascading and compounding consequences should also be considered.

Scenarios can also be used to explore the likely effect of responses to emerging risks. Game theory methods (see IEC 31010) can also be used to take into account the actions of other players (assumed to be acting in their own interests). For each scenario, the organization should consider the magnitude of the consequences to different objectives, their perceived likelihood and the uncertainties in these estimates.

If the initial estimates are highly uncertain, the possible options are to:

a) extend knowledge by consulting other experts or doing additional research;

b) acknowledge missing information by using a range for the likelihood of the risk occurrence (i.e. make the likelihood itself a stochastic variable);

c) use similar and better-understood information;

d) clearly communicate that knowledge can be based on limited information or individual perceptions, so that the decision-makers understand what their judgement will be based upon.

Evidence that is available to support estimates should be recorded (see 6.7).

Consequences and likelihood can be combined to give an estimate of a level of risk. However, independent information about possible consequences, and how likely they are, can sometimes be more valuable to those making decisions than combining this into a level of risk. Uncertainties in information and estimates should always be recorded and communicated.

There can be emerging risks where changes in context can be identified or early effects observed, but one or more of the following issues apply:

— there is no clear view of the possible scenarios;

— the relationship between cause and effect is unclear;

— the consequences and likelihood cannot be described or estimated;

— there is no way to grasp the full extent of the problem;

— no singular solution is available.

NOTE Such risks are sometimes referred to as “wicked risks”.

For these risks, the precautionary approach should be used, and controls should be specified in such a way that they can be updated as the situation becomes better defined. The organization should develop, so far as possible, the capability of anticipating, preparing, responding and adapting to unexpected consequences (see Clause 7) while continuing to seek information and data (see Clause 8). Identification of weak signals of change is particularly important for such risks.

As more data are gained, a description of scenarios, cause and effect relationships, estimates of consequence and likelihood, and other supporting information should be updated. Throughout this process, the perceived significance of an emerging risk can change significantly. Some emerging risks can prove insignificant, others can grow in importance. The developing understanding of possible scenarios can also lead to new risks being identified.

The time aspects relevant to the scenarios should be identified, as this will influence the urgency of further data collection and of treatment. Examples include the following:

— Short-term emerging risks are those that are already likely to have important consequences for the organization. These risks demand immediate attention, so resources should be allocated to data collection and analysis and further knowledge sought with urgency.

— Medium-term emerging risks are those where serious consequences are not expected in the short term, but can develop as the context changes. Knowledge building through effective interpretation of information is the key activity and can be used for the identification of possible controls that can take some time to action.

— Long-term emerging risks are not expected to have immediate consequences to objectives, but contexts can change and can give rise to significant risks in the future. For these risks, contexts are monitored and indicators that can identify the need to reconsider these risks are identified.

The rate of change is also relevant, such as, for example, the rate of change of:

— the organization’s context;

— the consequences;

— the risk intelligence throughout the risk intelligence cycle.

NOTE The risk intelligence maturity rate can be measured as “suitable quality of knowledge” (see Clause E.4).

As well as analysing the risks individually, the interactions between risks should be considered.

The effect of changed circumstances on risks that have been identified should also be explored. Assumptions that have been made should be reviewed in consideration of context changes to see whether these risks are evolving. Belief that controls will be effective in new circumstances are not always justified and should be tested or measured where possible.

6.4.4 Evaluating emerging risks

The results of analysis should be evaluated against the risk criteria. Social, regulatory, cultural, environmental and ethical aspects should also be considered. The significance of emerging risks should also be considered in business decisions and trade-offs where risk is involved.

For some risks, no immediate decisions about actions are required. Reasons for this include:

— there is insufficient information for any decision;

— the risks are judged to be of low significance for the organization;

— the time scale for any consequences is long.

Such risks should still be monitored.

Lack of data, information and knowledge about an emerging risk can result in significant uncertainty about consequences and how they can occur. It can be appropriate to take a precautionary approach when judging a risk's significance and deciding the response.

Perceptions of risk vary depending on people's objectives and biases. This is particularly the case for unfamiliar emerging risks and where there is often little data on which to base an assessment.

In some cases, where there is significant uncertainty regarding the potential consequences or their likelihood, it can be helpful to identify the possible actions and then consider which are practicable and useful. This approach is also used when the consequences being considered are extremely serious, such as the potential for fatalities.

As data on emerging risks are acquired, changes in a risk's perceived significance should be considered part of the organization's decision-making processes. In some cases, as knowledge increases, initial indicators of an emerging risk can prove to be unfounded. Priorities then change and monitoring can be reduced or possibly ended.

Information about risks considered significant should be communicated, if appropriate, throughout the organization so they can be taken into account in the decisions being made.

The organization should allocate responsibilities and authorities to detect and respond to changes in the available data and information about emerging risks and to communicate it to decision-makers.

6.5 Risk treatment

In the case of emerging risk, the changes that occur as the context evolves or as knowledge is gained can mean that the actions needed to manage the risk are also evolving. The effectiveness and efficiency of the treatments should therefore be continually evaluated and changes made, as necessary. Since consequences and likelihood are often unknown, the organization should develop the capability to anticipate, prepare for and respond to multiple unknowns, and adapt to unexpected situations.

In addition to ISO 31000:2018, 6.5, the following recommendations apply.

The organization should:

— analyse options for treating emerging risks;

NOTE Scenario analysis and event tree analysis can be useful for comparing different treatments, see IEC 31010.

— include emerging risks that can have serious consequences for its business continuity planning;

— remain agile, continually assessing its control context for both actions needed and resilience to unforeseen events;

— test the applied risk treatment measures;

— integrate plans to treat emerging risks into its operations and planning processes.

6.6 Monitoring and review

In addition to ISO 31000:2018, 6.6, the following recommendations apply.

The organization should devote effective and continual effort to monitoring and measuring risk management performance and reviewing the appropriateness of the framework, policy and plan for emerging risks.

The processes used to understand the context and assess the emerging risk should be monitored and periodically reviewed for effectiveness and improvement where appropriate.

Since emerging risks involve change, it is particularly important to continually monitor the outcomes of the process. For example, the organization should monitor the information about the context, the identified risks, the available data and information, the significance of the risk and the actions being taken. In this way, any occurring changes can be responded to promptly.

The organization should continually monitor the context for changing circumstances and their effects (see 6.3.1). The data and information available concerning an emerging risk should be monitored to update understanding regarding particular issues. Indicators that can flag when a change is beginning to occur should be identified, and these indicators should be monitored.

The effectiveness of existing controls and proposed treatments should also be monitored, as understanding of the risk improves, including a critical review of the results of previous relevant experience. The organization should put systems in place to learn from experience with the emerging risk as part of continual improvement.

6.7 Recording and reporting

In addition to ISO 31000:2018, 6.7, the following recommendations apply.

The information on emerging risk, the media used and how it is updated and reported on, depends on the needs of the organization and its stakeholders.

In general, records concerning the emerging risk should be used:

— to provide timely information on emerging risks to decision-makers;

— to provide assurance to stakeholders, both within and outside the organization, that emerging risks are being managed;

— to keep track of changes and historical data about emerging risks and their controls, as information is gained;

— to track progress against risk management plans and treatment plans.

The documented information on an emerging risk should contain descriptive information about the risk and the various potential scenarios (see Annex B). Verified quantitative information that assists understanding should be included in the documented information if available.

In the context of managing emerging risks, statutory or regulatory obligations in some jurisdictions can require independent reporting on managing emerging risks from designated functions or responsible persons within an organization. Documented information about emerging risks should be available, maintained and updated. An example of an emerging risks description or recording template is given in Annex B.

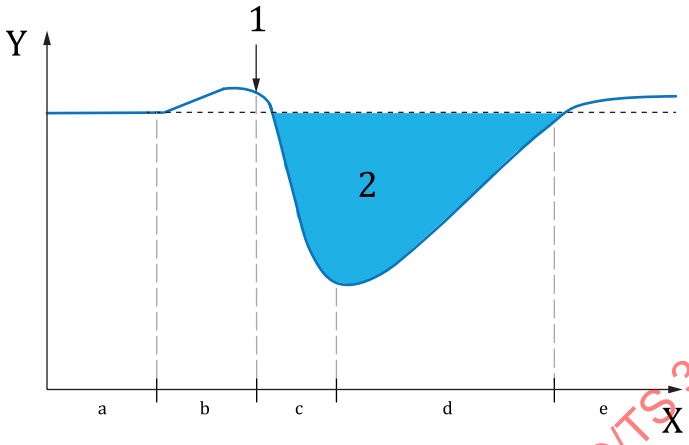
7 Enhancing resilience by managing emerging risks

7.1 Capability development

The application of the principles and process to managing emerging risks as provided in this document should help organizations to enhance their resilience capability by increasing their capacity to identify changes in a context that can represent weak signals or early warnings of potential emerging risks.

An organization's ability to anticipate, respond to and adapt to changing circumstances should be enhanced through collection of available data and analysis that supports meaningful interpretations of information and the essential knowledge for decision-making on emerging risks. The preparation of emerging risk scenarios based on available data and information should be used in order to provide a better understanding of the relationship between the development of the emerging risk and the extent

to which disruptive events can influence organizational functionality. The example in Figure 2 is based on a scenario that demonstrates the scale of loss and recovery of functionality along the dimensions of time from initial warnings of the emerging risk and the ability of an organization to anticipate, prepare and respond to the negative consequences of an emerging risk.



Key

X scenario time phase
Y functionality
1 onset of an emerging risk/event/scenario
2 loss of functionality
a Scanning for emerging risks.
b Anticipate/prepare.
c Absorb/withstand.
d Respond/recover.
e Adapt/transform.

NOTE Adapted from Reference [7]. Multiple scenarios are possible.

Figure 2 — Example of an emerging risk development scenario

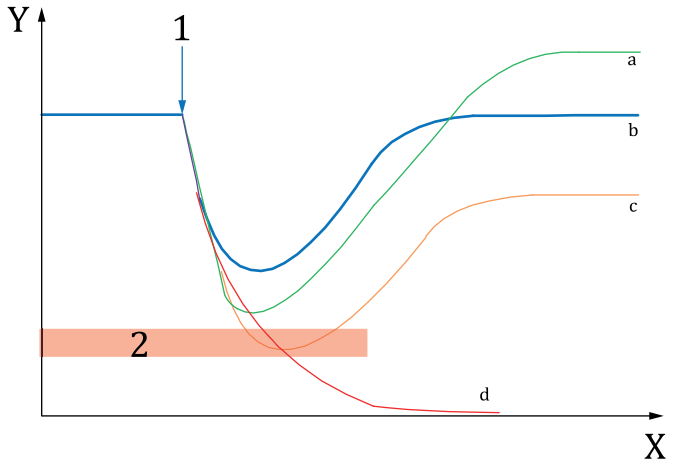
The resilience capabilities of an organization will determine the elapsed time between each phase to recovery from a disruptive event, with a corresponding impact upon the extent to which organizational functionality is lost and subsequently restored. The organization's ability to adapt and take advantage of changing circumstances can be reflected in increased functionality after the disruptive event. Figure 3 similarly demonstrates the relationship between the extent of loss and recovery from a disruptive event and the influence of resilience attributes and organizational capabilities on the following potential outcomes:

a) post-event functionality exceeding pre-existing conditions (adaptive capacity);

b) functionality restored to pre-existing conditions (continuity capacity);

c) pre-event functionality not fully restored (limited capability);

d) loss of minimum required functionality and system shutdown (inadequate capability).



Key

X scenario time
Y functionality
1 onset of an emerging risk/event/scenario
2 stress-test limits
a Functionality better than before.
b Functionality same as before.
c Functionality only partially recovered.
d Functionality completely lost.

NOTE Adapted from Reference [8].

Figure 3 — Potential impacts of an incident (event) on functionality

Continually scanning multiple contexts helps organizations better understand emerging risks and provide the knowledge required to build, measure and enhance organizational resilience attributes.

These organizational attributes can contribute to identifying and analysing emerging risks and any changes in their characteristics. This reduces the elapsed time from early warnings to initiation of a disruptive event, and enhances the agility of the organization to initiate a response and adapt to the changing circumstances. Resilience capability development/enhancement should be a proactive approach (e.g. stress testing the system to make improvements), see Reference [7].

A resilient organization (see Figure 3) should be able to absorb and adapt to a changing context, including changes that are potentially beneficial (e.g. in the case of a radical innovations or disruptive innovations). An organization should be prepared to anticipate, respond to and adapt to changes posed by such innovations, which can arise in the organization itself or in the market (e.g. to be capable to seize the opportunities offered by innovations to gain competitive advantages). Enhancing resilience should also be seen as a precautionary measure for unforeseeable risks.

7.2 Emerging risks and resilience indicators

Emerging risks can display characteristics that can impact an organization's ability to absorb and adapt in a changing context, and affect other aspects of the organization's resilience attributes, such as:

a) vision, purpose and core values;

b) decision-making on strategic issues;

c) leadership during periods of significant uncertainty;

d) culture of behaviour, creativity and innovation;

e) capacity to interpret information and apply knowledge;

f) allocation and deployment of resources;

g) networks and relationships;

h) coordination of disciplines involved in managing emerging risk;

i) ability to maintain the continual improvement of systems and processes.

Significant uncertainties concerning emerging risks also have the potential to change the context in which the above resilience attributes are developed, adopted and implemented. The extent to which changes in context can affect an organization's demonstrated ability to anticipate, plan, respond to and adapt to change is a lagging indicator of organizational resilience.

In order to evaluate its resilience prior to consequences from an emerging risk being detected, the organization should monitor its resilience attributes and stress test them by using exercises and tests for potential emerging risk scenarios. These scenarios can be formulated, for example, based on preliminary data analysis and continual scanning of multiple organizational contexts.

During and following a significant disruptive event related to emerging risk, the organization should evaluate the effectiveness of its resilience attributes with reference to Figure 3 and the following sample indicators of organizational resilience:

— time-dependent indicators:
  — elapsed time between a change in context and the recognition of an emerging risk;
  — elapsed time from an identification of risk and the occurrence of related events;
  — elapsed time from an emerging risk event to the commencement of loss of functionality;
  — duration of the impact on organizational objectives;
  — elapsed time from an event to returning to pre-existing conditions;
— productivity and performance indicators:
  — rate of loss of varying degrees of functionality;
  — extent of loss, expressed as a percentage of functionality;
  — duration of loss of functionality;
  — response to positive change to take advantage of an opportunity;
  — impact of a loss of functionality on organizational objectives;
— core resilience indicators:
  — sustainability of vision, goals, objectives and values;
  — extent of opportunities realized from emerging risks;
  — continual enhancement of capability to prepare, absorb, respond, recover and adapt/transform.

The organization should adopt resilience indicators, which can be agreed among its stakeholders, that:

— include values from any relevant source such as expert opinions (qualitative), measurements and big data (quantitative);

— enable benchmarking of resilience attributes of organizations (especially the key indicators) as agreed by relevant stakeholders;

— address the interoperability of communications and technical systems and their transparency across sector participants;

— describe resilience attributes comprehensively, clearly and without ambiguity.

The organization should apply resilience indicators to evaluate its resilience against emerging risks, and include them in the relevant risk scenarios, stress testing and exercise requirements. An example of a resilience indicator is given in Annex F.

8 Risk intelligence cycle and managing emerging risks

8.1 Overview

The sequence for obtaining intelligence for emerging risks and the process phases are shown in Figure 4. Intelligence itself can be conducted at different levels: strategic, tactical and operational. It should be applied to build and enhance knowledge regarding emerging risks.

A risk intelligence cycle should be applied to managing the emerging risk by:

— continual scanning to collect, analyse and interpret data, information and knowledge on emerging risks that occur within a context that is often characterized by unpredictable volatility, high degree of uncertainty, network complexity and rapid rates of change;

— considering that data on emerging risks gathered under such changing circumstances are limited (in quality and quantity) and their need for urgent interpretation often leads to increasing ambiguity of available information;

— considering data about other relevant known risks;

— associating the criticality of intelligence to effective decision-making due to the limitations of available data and information on emerging risks.

The effectiveness of the risk intelligent cycle, as well as its principles and process, is described in Annex E.

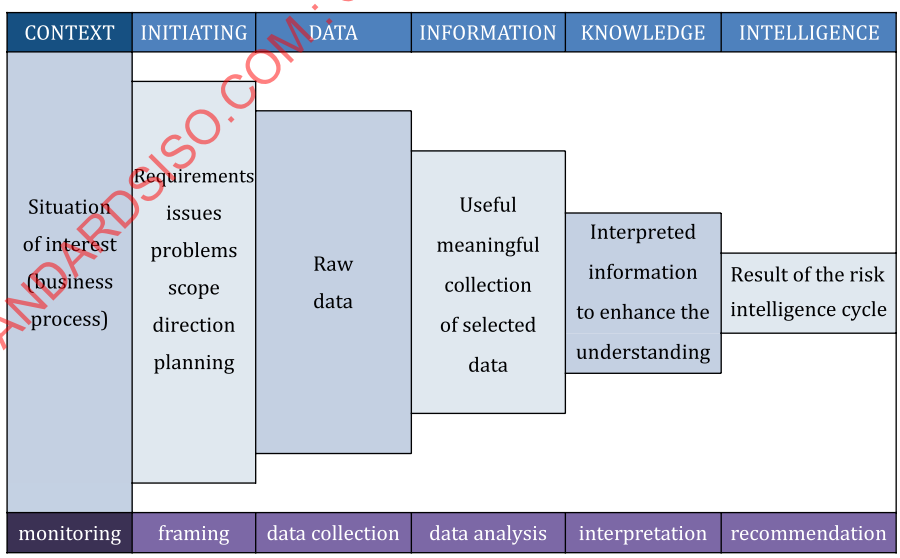
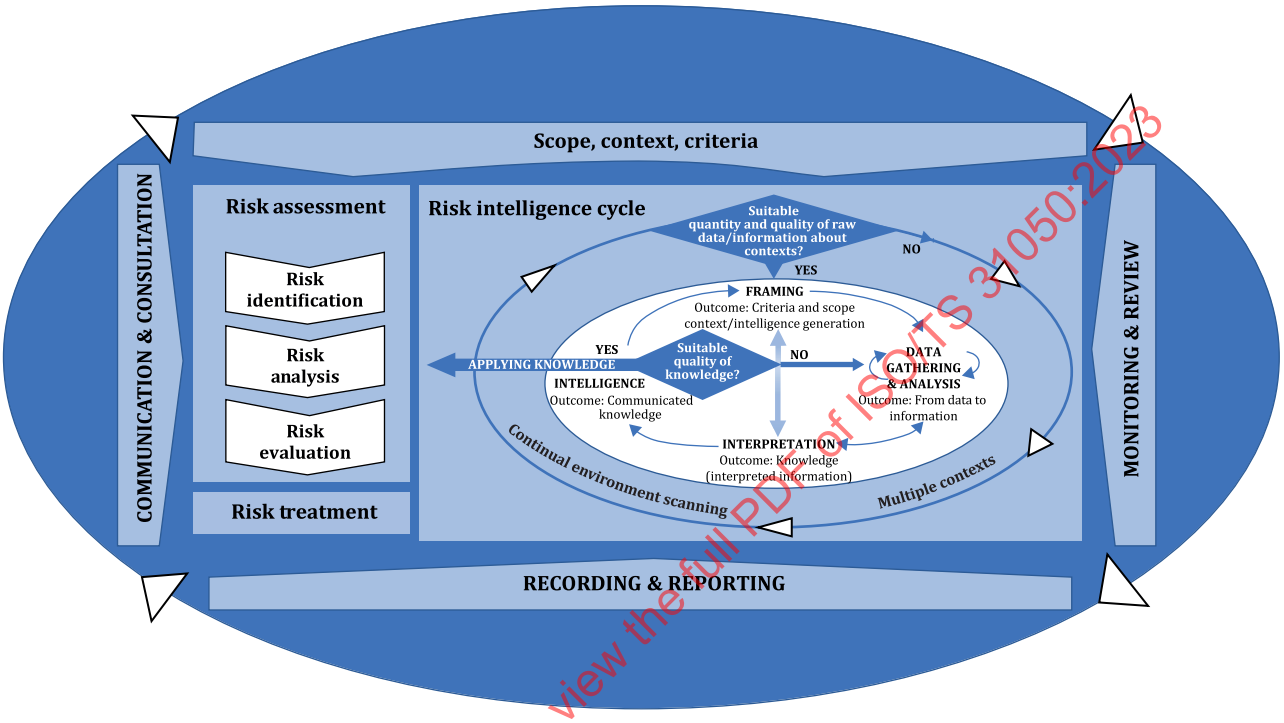


Figure 4 — Data, information, knowledge and intelligence (DIKI) process

8.2 Applying knowledge to decisions on emerging risks

The organization should apply the knowledge gained from the risk intelligence cycle at every step of the ISO 31000 risk management process relating to emerging risks. As confidence in the available data and information on the emerging risk increases, the quality of knowledge and intelligence will improve decision-making on emerging risks throughout each step of the ISO 31000 process (see Clause 6, Figure 5 and Figure E.1).



NOTE See the details in Figure E.1.

Figure 5 — Risk intelligence cycle for the emerging risk applied to the ISO 31000 process

Decision-makers, including top management and risk owners, should apply, on an ongoing basis, this intelligence in the risk management process to anticipate further changes in context and to make timely and informed decisions on strategy and planning for treating emerging risks. They should also recognize the importance of validating intelligence from knowledge accumulated on emerging risks. The inherent uncertainty in human judgements and the potential for cognitive bias from individual perceptions (see Annex D) should be considered when validating how information was converted to knowledge. This uncertainty reflects changing circumstances that can impact the decisions having unknown or uncertain outcomes.

An iterative approach should be applied to the DIKI process (see Figure 4) with verification at each step, as there are significant levels of uncertainty on emerging risks that can give rise to new questions requiring additional validation.

Applying the precautionary approach (see 6.4.4) in conjunction with the risk intelligence cycle enhances the effectiveness of managing emerging risks. In applying the knowledge cycle, collaboration and information sharing opportunities should be identified. The systems approach to managing the emerging risk should also consider interactions and interdependencies. Information should be shared with all stakeholders potentially affected by changes in the organizational context and information sharing with stakeholders directly affected by specific changes.

Annex A
(informative)

Examples of changes in context that can be sources of emerging risks

NOTE See References [9], [10] and [11].

The following changes in context can be sources of emerging risks:

— Natural hazards (extreme weather events): The United States Geological Survey published a study on a winter storm scenario[13], looking at the impact of an atmospheric river event (a global weather phenomenon bringing substantial amounts of rain or snow) with a predicted return period of 1 000 years. Findings indicate that flooding would overwhelm flood protections in many areas, resulting in the evacuation of more than a million residents, direct property damage of nearly USD 400 billion and business interruption costs of about USD 325 billion.

— Challenges of the internet of things (IoT) (cyber): The IoT will revolutionize the digital world. The digital revolution opens up a wide spectrum of opportunities for a resilient enterprise that is able to change its products, services and processes by making them smart, autonomous and connected. Such opportunities are, however, accompanied by the threats. Increased connectivity and reliance on digital processes raises questions about network and data security, resilience, long-term maintenance and software updates. Losses can occur from system malfunction and malicious attacks from hackers and criminals. There can also be legal and compliance risks due to the lack of consistent regulatory standards across countries.

— Antimicrobial drug resistance (health): Resistance occurs when microorganisms such as bacteria, viruses, fungi and parasites change in ways that render certain medications ineffective. When microorganisms become resistant to most antimicrobials, they are often referred to as “superbugs”. This is a major concern because a resistant infection can cause significant human and financial costs.

— Artificial intelligence (AI) lack of transparency: With progress in AI and cognitive computing, machines can begin to decide on behalf of humans. Decision transfer and lack of transparency or human oversight can result in unforeseen risks or unpredictable outcomes, creating complex liability issues. In addition, ethical, social and market aspects linked to AI are becoming more prominent.

— Autonomous machines (cyber, AI): Due to new developments in mechatronics, speed learning and AI, there has been rapid progress in autonomous machines, affecting most industries, the military and everyday life. Autonomous vehicles are particularly well publicized, and this will likely change the risk landscape for various lines of insurance business.

— Climate change transition risk (climate): Transition risks arise as the world aims to adapt to the warming climate and reduce the emission of greenhouse gases (especially CO_2). This has implications for insurers in product design and associated liabilities, as well as in the way they invest. One particular transition risk is the occurrence of stranded assets. These are assets that become obsolete due to policy changes (e.g. coal sector, diesel vehicles) or due to carbon pricing (e.g. surplus aircraft).

Annex B
(informative)

Example of emerging risks description or recording template

The examples and lists provided in this annex are not comprehensive, limiting or prescriptive. The information continually acquired for an emerging risk should contain:

a) clear identification of the emerging risk notion (e.g. an automatically assigned identification (ID) code);

b) metadata related to the origin: author, time, organization, etc.;

c) name of the emerging risk notion;

d) description (the risk story) of possible scenarios, including interconnection with other risks;

e) the pre-assessment results related to:

   1) impact characteristics, both positive and negative (e.g. systemic, cumulative, serial loss, potential benefits);

   2) geographical and temporal data (where and when the risk appeared);

   3) governance, communication, policies, technology, etc.;

   4) phases of the life cycle (which phase, e.g. end-of-life);

   5) areas of human activity affected (e.g. energy, transportation);

   6) possible economic and other impacts (positive and negative);

   7) risk owner(s);

   8) knowledge strength (emergence and maturity);

   9) assessment methods and tools possibly applicable;

   10) assessment guidelines or regulations, if any;

   11) possible indicators of risk and resilience;

f) assessment information and assessment results, including:

   1) sources and interconnectedness of the emerging risk and potential scenarios;

   2) a description and, where appropriate, the magnitude of consequences (positive and negative);

   3) the effectiveness and efficiency of relevant controls already in place;

   4) information about the likelihood/plausibility of occurrence (of scenarios and consequences);

   5) potential time scales, velocity and rate of change;

   6) reference to documents and sources of information on which analysis is based;

   7) opportunities and threats that can be identified in the changing context;

   8) analysis methods and tools used and reference to reports of their outputs;

9) uncertainties in the analysis of data and the interpretation of information;

10) possible weak signals or early indicators that change is occurring;

g) treatment actions recommended, including time scales and responsibilities;

h) residual risk;

i) arrangements for monitoring the context and updating information on emerging risks;

j) references and related preceding cases and knowledge;

k) reference to documents providing more detail.

Annex C
(informative)

Systemic risks

Many emerging risks are systemic in that they originate and evolve in the nexus of tightly coupled dynamic systems, which is one of the main characteristics of contemporary pluralistic societies. The term "systemic risk" highlights the interconnectivity of threats that organizations face today. The Organisation for Economic Co-operation and Development (OECD) chose the category of systemic risks to account for emerging risks that threaten society's essential systems, such as infrastructure, health care and telecommunications. Systemic risks refer to risk phenomena that propagate from the regional to the national and global level.

Systemic risks can be differentiated from other types of risks by the following five attributes.

a) A high level of complexity characterizes systemic risks. Causal processes are difficult to understand when it comes to analysing systemic risks. On the one hand, this is due to the inherent complexities of the systems under consideration (e.g. critical infrastructures, corporations, ecosystems and their components). On the other hand, complexity is caused by the fact that systemic risks can combine with conventional risks (e.g. natural hazards).

b) Systemic risks are transboundary and trans-sectoral. Although their origins can be traced back to one specific system and/or incident, their ripple effects spread out towards other systems where they cause further impacts. Therefore, they challenge conventional risk analysis and governance approaches, often based on compartmentalization and fragmentation.

c) Systemic risks develop in a non-linear manner due to their non-deterministic cause-effect relationships. Systemic risks are characterized by a combination of known factors and unknown triggers or promoters that evolve randomly or which are at the limit of calculability.

d) Many systemic risks are characterized by non-linear relationships typically associated with tipping points or tipping periods. Once a tipping point is reached, the affected systems drastically change their conditions of existence in a short time.

e) There is often a lag in regulation and public perception about the potentially devastating impacts of systemic risks. Some systemic risks, such as climate change, have received public attention, yet policies to manage systemic risks are often perceived as piecemeal, insufficient and incoherent by stakeholders and the public.

Organizations should pay attention to these properties of systemic risks, most notably:

— the interdependencies;

— the complex structure of intervening factors, uncertainties and non-linear relationships which requires a systems approach for managing emerging risks.

Organizations should prepare for unforeseen stressors of emerging risks and for the fact that emerging risks can cause cascading or compounding effects. Effective, integrative and inclusive governance strategies are necessary to pursue the goals of preventing, mitigating or coping with systemic threats. In particular, the concerns of stakeholders or the public should be considered in the risk assessment as well as the risk management process.

Annex D
(informative)

Example factors that can influence managing emerging risks

NOTE See References [7] and [12].

Table D.1 — Example factors that can influence managing emerging risks

Factor	Concise explanation and comment
Related to general perception and communication	
Misperception and misinterpretation	Possible misperception of opportunities or benefits. Susceptibility to deliberate or other misinterpretation.
False positives	Influence of false positives on assessment result.
False negatives	Influence of false negatives on assessment result.
(Global) Catastrophic potential	If fatalities occur in large numbers in a single event, instead of in small numbers dispersed over time, the perception of risk rises.
Sensitivity	Sensitivity of risk perception on single events (e.g. accidents), volatility of public perception.
Miscommunication	Communication of emerging risks can be a factor in the perception of the risk level, as by definition the available knowledge is weak. In extreme cases, the miscommunication can be a risk of its own.
Single person level perception	
Lack of familiarity	Unfamiliar or novel risks can make a person worry more.
Lack of understanding	If a person believes that how an activity or technology works is not well understood, their sense of risk goes up.
Lack of personal control or voluntariness	If a person feels the potential for harm is beyond their control (e.g. as a passenger in an airplane), they worry more than if they feel that they are in control (e.g. as the driver of a car). If they cannot decide personally to engage with the risk or not, the risk feels more threatening.
Involvement of or risk for future generations	If the risk involves future generations, a person tends to find it more relevant and subject to social amplification.
Identity of affected persons	Identifiable people who are affected by the consequences of risk rather than statistical abstractions make the sense of risk rise.
Dread	If the effects generate fear, the sense of risk rises.
Lack of trust	If the institutions involved are not trusted, personal risk perception generally rises.
Lack of equity	If the benefits go to some people and the downside outcomes to other people, the risk ranking is raised.
Lack of reversibility	If the effects of an outcome cannot be reversed, the risk rises.
Personal risk	If the risk is a personal risk (involuntary), a person tends to perceive the risk as higher (unless they think they are in better control than the average person).
Cognitive biases	Biases such as confirmation bias, and other cognitive biases including information fatigue(s), can significantly influence emerging risks and their perception.

Table D.1 *(continued)*

Factor	Concise explanation and comment
Related to the governance of emerging risks	
Authorization	Availability of authorization or certification schemes (progressive authorization).
Mapping	Possibility to map (e.g. on geographical or context maps).
Management	Possibility to manage, especially consequences.
Protection or precaution	Possibility to envisage the implementation of protective or precautionary measures.
Social unrest	Potential to provoke or result in social unrest.
Related to the global management of emerging risks	
Lack of possibility to observe or monitor	Possibility to monitor the risk if false signals resulting from monitoring are very high.
Lack of possibility for control or mitigation	Lack of inherent management, control or planned mitigation mechanisms.
Susceptibility to ignorance	The complexity of the modern world often leads to the situation in which people are flooded with information about a phenomenon or an issue (e.g. computers), but the basic understanding of the phenomenon is missing.