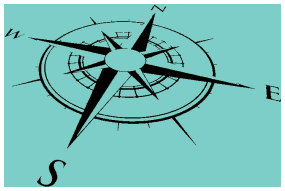
Risk management — Vocabulary

This Guide provides basic vocabulary to develop common understanding on risk management concepts and terms among organizations and functions, and across different applications and types.

In addition to managing threats to the achievement of their objectives, organizations are increasingly applying risk management processes and developing an integrated approach to risk management in order to improve the management of potential opportunities. The terms and definitions in this Guide are, therefore, broader in concept and application than those contained in ISO/IEC Guide 51, which is confined to safety aspects of risk, i.e. with undesirable or negative consequences. Since organizations increasingly adopt a broader approach to the management of risk, this Guide addresses all applications and sectors. This Guide is generic and is compiled to encompass the general field of risk management. The terms are arranged in the following order:

- terms relating to risk;
- terms relating to risk management;
- terms relating to the risk management process;
- terms relating to communication and consultation;
- terms relating to the context;
- term relating to risk assessment;
- terms relating to risk identification;
- terms relating to risk analysis;
- terms relating to risk evaluation;
- terms relating to risk treatment;
- terms relating to monitoring and measurement.

Contents



International Organization for Standardization (ISO)

Description:

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.

Stakeholder(s):

Risk Managers :
This Guide is intended to be used by:

- *those engaged in managing risks,*
- *those who are involved in activities of ISO and IEC, and*
- *developers of national or sector-specific standards, guides, procedures and codes of practice relating to the management of risk.*

Vision

Mutual and consistent understanding of, and a coherent approach to, the description of activities relating to the management of risk, and the use of uniform risk management terminology in processes and frameworks dealing with the management of risk

Mission

To develop common understanding on risk management concepts and terms

1. Risks

[Define] risks

Terms relating to risk

1.1. Objectives

[Determine the] effects of uncertainties on objectives

risk ~ effect of uncertainty on objectives Note 1 to entry: An effect is a deviation from the expected — positive and/or negative. Note 2 to entry: Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process). Note 3 to entry: Risk is often characterized by reference to potential events (3.5.1.3) and consequences (3.6.1.3), or a combination of these. Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood (3.6.1.1) of occurrence. Note 5 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

2. Management

Manage risks

Terms relating to risk management

2.1. Activities

Coordinate activities to direct and control organizations with regard to risks

risk management ~ coordinated activities to direct and control an organization with regard to risk (1.1)

2.1.1. Framework

[Identify the] components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management

risk management framework ~ set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring (3.8.2.1), reviewing and continually improving risk management (2.1) throughout the organization Note 1 to entry: The foundations include the policy, objectives, mandate and commitment to manage risk (1.1). Note 2 to entry: The organizational arrangements include plans, relationships, accountabilities, resources, processes and activities. Note 3 to entry: The risk management framework is embedded within the organization's overall strategic and operational policies and practices.

2.1.2. Policy

State the intentions and directions related to risk management

risk management policy ~ statement of the overall intentions and direction of an organization related to risk management (2.1)

2.1.3. Plan

Specify the approach, management components and resources to be applied to the management of risks

risk management plan ~ scheme within the risk management framework (2.1.1) specifying the approach, the management components and resources to be applied to the management of risk (1.1) Note 1 to entry: Management components typically include procedures, practices, assignment of responsibilities, sequence and timing of activities. Note 2 to entry: The risk management plan can be applied to a particular product, process and project, and part or whole of the organization.

3. Processes

[Institute] risk management processes

Terms relating to the risk management process

3.1. Policies, Procedures & Practices

Apply management policies, procedures and practices

risk management process ~ systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring (3.8.2.1) and reviewing risk (1.1)

3.2. Communication & Consultation

Communicate and consult with stakeholders

Terms relating to communication and consultation.

3.2.1. Information & Dialogue

Provide, share or obtain information and engage in dialogue with stakeholders

communication and consultation ~ continual and iterative processes that an organization conducts to provide, share or obtain information, and to engage in dialogue with stakeholders (3.2.1.1) regarding the management of risk (1.1) Note 1 to entry: The information can relate to the existence, nature, form, likelihood (3.6.1.1), significance, evaluation, acceptability and treatment of the management of risk. Note 2 to entry: Consultation is a two-way process of informed communication between an organization and its stakeholders on an issue prior to making a decision or determining a direction on that issue. Consultation is: — a process which impacts on a decision through influence rather than power; and — an input to decision making, not joint decision making.

3.2.1.1. Stakeholders

[Identify] persons and organizations that can affect, be affected by, or perceive themselves to be affected by decisions and activities

stakeholder ~ person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity Note 1 to entry: A decision maker can be a stakeholder.

3.2.1.2. Perception

[Take into account] stakeholder views on risks

risk perception ~ stakeholder's (3.2.1.1) view on a risk (1.1) Note 1 to entry: Risk perception reflects the stakeholder's needs, issues, knowledge, belief and values.

3.3. Context

Establish the contexts in which risks occur

Terms relating to the context

3.3.1. Parameters

Define the external and internal parameters to be taken into account

establishing the context ~ defining the external and internal parameters to be taken into account when managing risk, and setting the scope and risk criteria (3.3.1.3) for the risk management policy (2.1.2)

3.3.1.1. External Factors

[Consider the] external environments in which organizations seek to achieve their objectives

external context ~ external environment in which the organization seeks to achieve its objectives Note 1 to entry: External context can include: — the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local; — key drivers and trends having impact on the objectives of the organization; and — relationships with, and perceptions and values of external stakeholders (3.2.1.1).

3.3.1.2. Internal Factors

[Consider the] internal environments in which organizations seek to achieve their objectives

internal context ~ internal environment in which the organization seeks to achieve its objectives Note 1 to entry: Internal context can include: — governance, organizational structure, roles and accountabilities; — policies, objectives, and the strategies that are in place to achieve them; — the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies); — information systems, information flows and decision-making processes (both formal and informal); — relationships with, and perceptions and values of internal stakeholders; — the organization's culture; — standards, guidelines and models adopted by the organization; and — form and extent of contractual relationships.

3.3.1.3. Criteria

[Specify the] terms of reference against which the significance of risks is evaluated

risk criteria ~ terms of reference against which the significance of a risk (1.1) is evaluated Note 1 to entry: Risk criteria are based on organizational objectives, and external (3.3.1.1) and internal context (3.3.1.2). Note 2 to entry: Risk criteria can be derived from standards, laws, policies and other requirements.

3.4. Assessment

Assess risks

Term relating to risk assessment

3.4.1. Identification, Analysis & Evaluation

Identify, analyze, and evaluate risks

risk assessment ~ overall process of risk identification (3.5.1), risk analysis (3.6.1) and risk evaluation (3.7.1)

3.5. Identification

Identify risks

Terms relating to risk identification

3.5.1. Discovery, Recognition & Description

Find, recognize and describe risks

risk identification ~ process of finding, recognizing and describing risks (1.1) Note 1 to entry: Risk identification involves the identification of risk sources (3.5.1.2), events (3.5.1.3), their causes and their potential consequences (3.6.1.3). Note 2 to entry: Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholder's (3.2.1.1) needs.

3.5.1.1. Statement

[Provide a] structured statement of risk

risk description ~ structured statement of risk usually containing four elements: sources, events (3.5.1.3), causes and consequences (3.6.1.3)

3.5.1.2. Sources

[Identify] elements potentially posing risks

risk source ~ element which alone or in combination has the intrinsic potential to give rise to risk (1.1) Note 1 to entry: A risk source can be tangible or intangible.

3.5.1.3. Events

[Identify] circumstances that create risks

event ~ occurrence or change of a particular set of circumstances Note 1 to entry: An event can be one or more occurrences, and can have several causes. Note 2 to entry: An event can consist of something not happening. Note 3 to entry: An event can sometimes be referred to as an “incident” or “accident”. Note 4 to entry: An event without consequences (3.6.1.3) can also be referred to as a “near miss”, “incident”, “near hit” or “close call”.

3.5.1.4. Hazards

[Identify] sources of potential harm

hazard ~ source of potential harm Note 1 to entry: Hazard can be a risk source (3.5.1.2).

3.5.1.5. Managers

[Identify the] persons and entities with accountability and authority to manage risks

risk owner ~ person or entity with the accountability and authority to manage a risk (1.1)

Stakeholder(s):

Risk Owners **Risk Managers**

3.6. Analysis

Analyze risks

Terms relating to risk analysis

3.6.1. Attributes & Levels

Comprehend the nature of and determine the levels of risks

risk analysis ~ process to comprehend the nature of risk (1.1) and to determine the level of risk (3.6.1.8) Note 1 to entry: Risk analysis provides the basis for risk evaluation (3.7.1) and decisions about risk treatment (3.8.1). Note 2 to entry: Risk analysis includes risk estimation.

3.6.1.1. Likelihood

[Determine the] chances of happenings

likelihood ~ chance of something happening Note 1 to entry: In risk management terminology, the word “likelihood” is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically [such as a probability (3.6.1.4) or a frequency (3.6.1.5) over a given time period]. Note 2 to entry: The English term “likelihood” does not have a direct equivalent in some languages; instead, the equivalent of the term “probability” is often used. However, in English, “probability” is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, “likelihood” is used with the intent that it should have the same broad interpretation as the term “probability” has in many languages other than English.

3.6.1.2. Exposures

[Determine the] extent to which organizations and stakeholders are subject to events

exposure ~ extent to which an organization and/or stakeholder (3.2.1.1) is subject to an event (3.5.1.3)

3.6.1.3. Consequences

[Determine the] outcomes of events affecting objectives

consequence ~ outcome of an event (3.5.1.3) affecting objectives Note 1 to entry: An event can lead to a range of consequences. Note 2 to entry: A consequence can be certain or uncertain and can have positive or negative effects on objectives. Note 3 to entry: Consequences can be expressed qualitatively or quantitatively. Note 4 to entry: Initial consequences can escalate through knock-on effects.

3.6.1.4. Probability

[Determine the] the chances of occurrences

probability ~ measure of the chance of occurrence expressed as a number between 0 and 1, where 0 is impossibility and 1 is absolute certainty Note 1 to entry: See definition 3.6.1.1, Note 2.

3.6.1.5. Frequencies

[Determine the] numbers of events and outcomes per defined units of time

frequency ~ number of events (3.5.1.3) or outcomes per defined unit of time Note 1 to entry: Frequency can be applied to past events (3.5.1.3) or to potential future events, where it can be used as a measure of likelihood (3.6. 1.1)/probability (3.6.1.3).

3.6.1.6. Vulnerabilities

[Identify] intrinsic properties resulting in susceptibilities to risk sources

vulnerability ~ intrinsic properties of something resulting in susceptibility to a risk source (3.5.1.2) that can lead to an event with a consequence (3.6.1.3)

3.6.1.7. Matrix

Rank and display risks

risk matrix ~ tool for ranking and displaying risks (1.1) by defining ranges for consequence (3.6.1.3) and likelihood (3.6.1.1)

3.6.1.8. Levels

[Determine the] magnitude of risks and combinations of risks

level of risk ~ magnitude of a risk (1.1) or combination of risks, expressed in terms of the combination of consequences (3.6.1.3) and their likelihood (3.6.1.1)

3.7. Evaluation

Evaluate risks

3.7 Terms relating to risk evaluation

3.7.1. Comparison

Compare the results of risk analyses with risk criteria

risk evaluation ~ process of comparing the results of risk analysis (3.6.1) with risk criteria (3.3.1.3) to determine whether the risk (1.1) and/or its magnitude is acceptable or tolerable Note 1 to entry: Risk evaluation assists in the decision about risk treatment (3.8.1).

3.7.1.1. Attitudes

[Determine] organizational approaches to assess and pursue, retain, take or turn away from risks

risk attitude ~ organization's approach to assess and eventually pursue, retain, take or turn away from risk (1.1)

3.7.1.2. Appetites

[Evaluate the] amounts and types of risks that organizations are willing to accept

risk appetite ~ amount and type of risk (1.1) that an organization is willing to pursue or retain

3.7.1.3. Tolerances

[Evaluate] readiness to bear risks after treatment in order to achieve objectives

risk tolerance ~ organization's or stakeholder's (3.2.1.1) readiness to bear the risk (1.1) after risk treatment (3.8. 1) in order to achieve its objectives Note 1 to entry: Risk tolerance can be influenced by legal or regulatory requirements.

3.7.1.4. Aversions

Turn away from risks

risk aversion ~ attitude to turn away from risk (1.1)

3.7.1.5. Aggregation

Combine risks to develop more complete understanding

risk aggregation ~ combination of a number of risks into one risk (1.1) to develop a more complete understanding of the overall risk

3.7.1.6. Acceptance

[Make] informed decisions to take particular risks

risk acceptance ~ informed decision to take a particular risk (1.1) Note 1 to entry: Risk acceptance can occur without risk treatment (3.8.1) or during the process of risk treatment. Note 2 to entry: Accepted risks are subject to monitoring (3.8.2.1) and review (3.8.2.2).

3.8. Treatment

Treat risks

Terms relating to risk treatment

3.8.1. Modifications

Modify risks

risk treatment ~ process to modify risk (1.1) Note 1 to entry: Risk treatment can involve: — avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk; — taking or increasing risk in order to pursue an opportunity; — removing the risk source (3.5.1.2); — changing the likelihood (3.6.1.1); — changing the consequences (3.6.1.3); — sharing the risk with another party or parties [including contracts and risk financing (3.8.1.4)]; and — retaining the risk by informed decision. Note 2 to entry: Risk treatments that deal with negative consequences are sometimes referred to as “risk mitigation”, “risk elimination”, “risk prevention” and “risk reduction”. Note 3 to entry: Risk treatment can create new risks or modify existing risks.

3.8.1.1. Controls

Take measures to modify risks

control ~ measure that is modifying risk (1.1) Note 1 to entry: Controls include any process, policy, device, practice, or other actions which modify risk. Note 2 to entry: Controls may not always exert the intended or assumed modifying effect.

3.8.1.2. Avoidance

[Decide] not to be involved in, or to withdraw from, activities in order not to be exposed to particular risks

risk avoidance ~ informed decision not to be involved in, or to withdraw from, an activity in order not to be exposed to a particular risk (1.1) Note 1 to entry: Risk avoidance can be based on the result of risk evaluation (3. 7.1) and/or legal and regulatory obligations.

3.8.1.3. Sharing

Distribute risks among parties

risk sharing ~ form of risk treatment (3.8.1) involving the agreed distribution of risk (1.1) with other parties Note 1 to entry: Legal or regulatory requirements can limit, prohibit or mandate risk sharing. Note 2 to entry: Risk sharing can be carried out through insurance or other forms of contract. Note 3 to entry: The extent to which risk is distributed can depend on the reliability and clarity of the sharing arrangements. Note 4 to entry: Risk transfer is a form of risk sharing.

3.8.1.4. Financing

Arrange for funding to meet or modify financial consequences

risk financing ~ form of risk treatment (3.8.1) involving contingent arrangements for the provision of funds to meet or modify the financial consequences (3.6.1.3) should they occur

3.8.1.5. Retentions

[Determine the degrees of] acceptance of the potential benefits of gain, or burdens of losses, from particular risks

risk retention ~ acceptance of the potential benefit of gain, or burden of loss, from a particular risk (1.1) Note 1 to entry: Risk retention includes the acceptance of residual risks (3.8.1.6). Note 2 to entry: The level of risk (3.6. 1.8) retained can depend on risk criteria (3.3.1.3).

3.8.1.6. Residuals

[Identify the] risks remaining after treatments

residual risk ~ risk (1.1) remaining after risk treatment (3.8.1) Note 1 to entry: Residual risk can contain unidentified risk. Note 2 to entry: Residual risk can also be known as “retained risk”.

3.8.1.7. Resilience

Adapt to complex and changing environments

resilience ~ adaptive capacity of an organization in a complex and changing environment

3.8.2. Monitoring & Measurement

Monitor and measure risks

Terms relating to monitoring and measurement

3.8.2.1. Monitoring

Continuously observe deviations from expected performance levels

monitoring ~ continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected Note 1 to entry: Monitoring can be applied to a risk management framework (2.1.1), risk management process (3.1), risk (1.1) or control (3.8.1.1).

3.8.2.2. Reviews

Determine the suitability, adequacy and effectiveness of subject matters to achieve objectives

review ~ activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives Note 1 to entry: Review can be applied to a risk management framework (2.1.1), risk management process (3.1), risk (1.1) or control (3.8.1.1).

3.8.2.3. Reports

Provide information on the state and management of risks

risk reporting ~ form of communication intended to inform particular internal or external stakeholders (3.2.1.1) by providing information regarding the current state of risk (1.1) and its management

3.8.2.4. Register

Record information about risks

risk register ~ record of information about identified risks (1.1) Note 1 to entry: The term “risk log” is sometimes used instead of “risk register”.

3.8.2.5. Profiles

Describe sets of risks

risk profile ~ description of any set of risks (1.1) Note 1 to entry: The set of risks can contain those that relate to the whole organization, part of the organization, or as otherwise defined.

3.8.2.6. Audits

Obtain and evaluate evidence to determine the adequacy and effectiveness of risk management frameworks

risk management audit ~ systematic, independent and documented process for obtaining evidence and evaluating it objectively in order to determine the extent to which the risk management framework (2.1.1), or any selected part of it, is adequate and effective.

Administrative Information

Start Date:
End Date:

Publication Date: 2020-05-19
Source: https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en

Submitter:

Given Name: **Surname:** Ambur
Email: Owen.Ambur@verizon.net
Phone: