ISO/TMB WG on Risk management N 066

Date: 2008-04-01

ISO/IEC CD 2 Guide 73

ISO/TMB WG on Risk management

Risk management — Vocabulary

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: Guide
Document subtype:
Document stage: (30) Committee
Document language:E

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

Draft Guides adopted by the responsible Committee or Group are circulated to national bodies for voting. Publication as a Guide requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC Guide 73 was prepared by ISO TMB Working Group on Risk Management.

Introduction

Organizations of all types and sizes face a range of risks that can affect the achievement of their objectives.

These objectives can relate to a range of the organization's activities, from strategic initiatives to its operations, processes and projects, and be reflected in terms of strategic, operational, financial and reputational outcomes and impacts.

All activities of an organization involve risks. Risk management aids decision making by taking account of uncertainty and its effect on achieving objectives and assessing the need for any actions.

Risk management process involves applying logical and systematic methods for:

— communication and consultation throughout the process;

— establishing the context;

— identifying, analyzing, evaluating and treating risk associated with any activity, process, function, project, product, service or asset;

— monitoring and reviewing risk; and

— recording and reporting the results appropriately.

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

This Guide is generic and is compiled to encompass the general field of risk management.

When using risk management terminology, the definitions in this Guide should be given first consideration.

Risk management — Vocabulary

1 Scope

This Guide provides the definitions of generic terms related to risk management. This Guide aims to encourage a mutual and consistent understanding, a coherent approach to the description of activities relating to the management of risk, and use of uniform risk management terminology in processes and frameworks dealing with the management of risk.

This Guide is intended to be used by:

— those engaged in managing risks in practice;

— 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.

For principles and guidelines on the implementation of risk management, reference is made to ISO 31000.

2 Overview of risk management terms and definitions

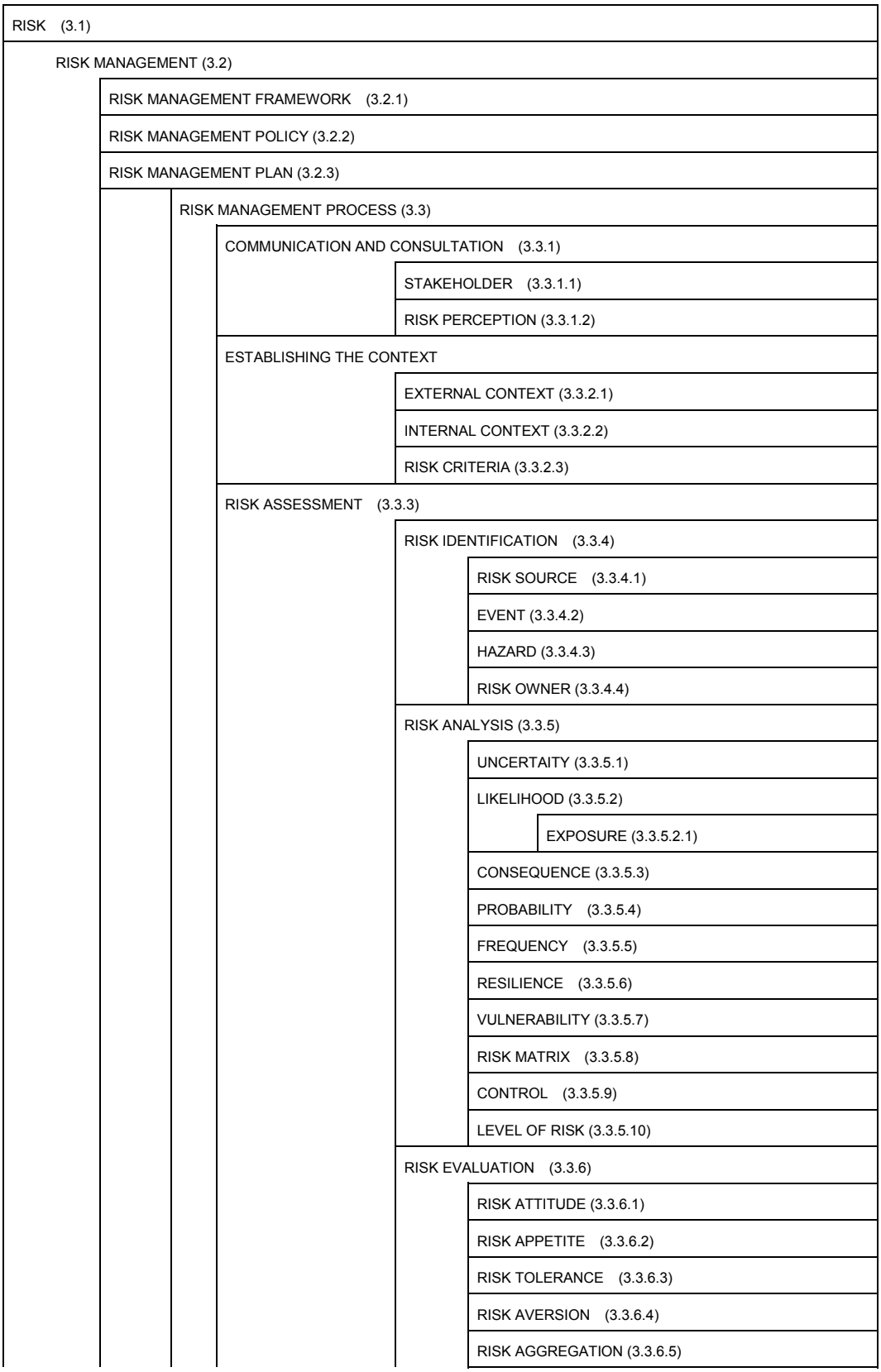
Risk management is application specific. In some circumstances, it can be necessary to supplement the vocabulary in this Guide. Where terms related to the management of risk are used in a standard, it is imperative that their intended meanings within the context of the standard are not misinterpreted, misrepresented or misused.

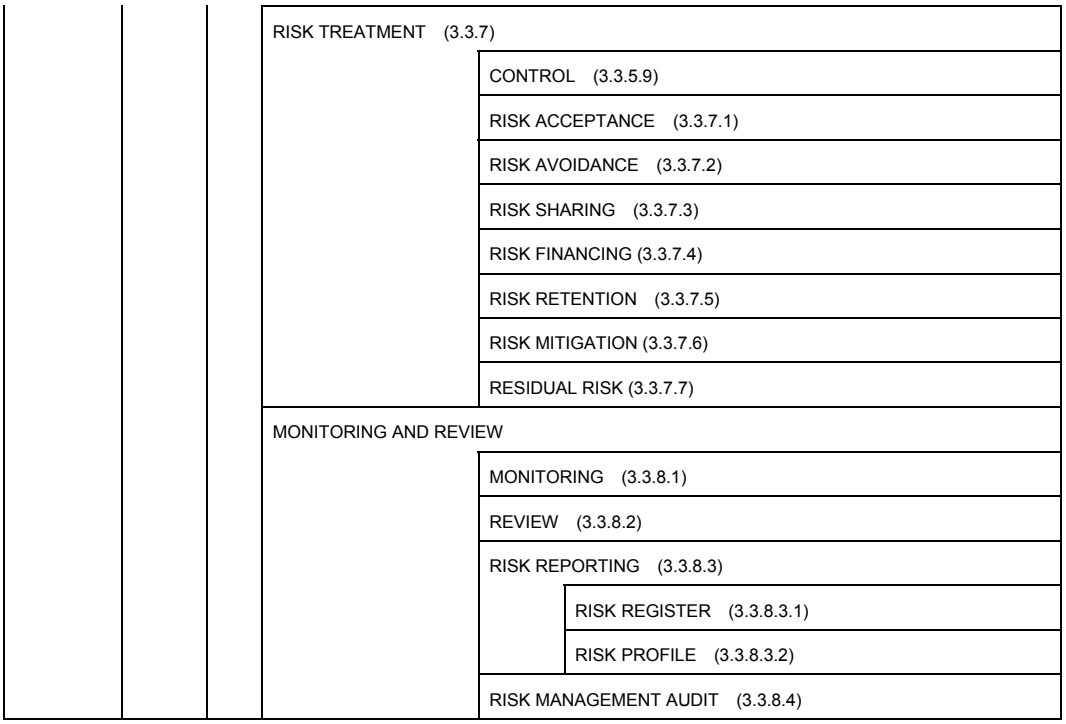
In addition to managing threats to their objectives, organizations are increasingly applying risk management processes and developing an integrated approach to risk management in order to improve the management of potential opportunities. The terms and definitions in this Guide are, therefore, broader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

The relationship between the terms for risk management is shown in Figures 1.

NOTE When a term which is defined in this Guide is cited in another definition, it is given in boldface with its cross-reference. Terms cited in the notes are in boldface but without cross-references.

81





82 **Figure 1 — Relationship between terms based on their definitions regarding risk management**

3 Terms and definitions

3.1
risk
effect of **uncertainty** (3.3.5.1) on objectives

NOTE 1 An effect is a deviation from the expected - positive and/or negative.

NOTE 2 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 Risk is often characterized by reference to potential **events**, **consequences**, or a combination of these and how they can affect the achievement of objectives.

NOTE 4 Risk is often expressed in terms of a combination of the **consequences** of an **event** or a change in circumstances, and the associated **likelihood** of occurrence.

3.2
risk management
coordinated activities to direct and control an organization with regard to **risk** (3.1)

3.2.1
risk management framework
set of components that provide the foundations and organizational arrangements for designing, implementing, **monitoring** (3.3.8.1), reviewing and continually improving **risk management processes** (3.3) throughout the organization

NOTE 1 The foundations include the policy, objectives, mandate and commitment to manage **risk**.

NOTE 2 The organizational arrangements include plans, relationships, accountabilities, resources, processes and activities.

NOTE 3 The risk management framework is embedded within the organization's overall strategic and operational policies and practices.

3.2.2
risk management policy
overall intentions and direction of an organization related to **risk management** (3.2)

3.2.3
risk management plan
document within the **risk management framework** (3.2.1) specifying the approach, the management components and resources to be applied to the management of **risk** (3.1)

NOTE 1 Management components typically include procedures, practices, assignment of responsibilities and sequence of activities.

NOTE 2 The risk management plan can be applied to a particular product, process and project, and part or whole of the organization.

3.3
risk management process
systematic application of management policies, procedures and practices to the tasks of communicating, consulting, establishing the context, identifying, analyzing, evaluating, treating, **monitoring** (3.3.8.1) and reviewing **risk** (3.1)

3.3.1
communication and consultation
continual or iterative processes that an organization conducts to provide, share or obtain information and to engage in dialogue with **stakeholders** (3.3.1.1) regarding the management of **risk** (3.1)

NOTE 1 The information can relate to the existence, nature, form, **likelihood**, severity, evaluation, acceptability, treatment or other aspects of the management of **risk**.

NOTE 2 Consultation is a process of informed communication between organization and its **stakeholders** on an issue prior to making a decision or determining a direction on a particular issue. Consultation is:

— a process not an outcome which impacts on a decision through influence rather than power; and

— about inputs to decision making, not joint decision making.

NOTE 3 Internal communication and consultation should be appropriately recorded.

3.3.1.1
stakeholder
any person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

NOTE A decision maker is also a stakeholder.

3.3.1.2
risk perception
stakeholder's (3.3.1.1) view on a **risk** (3.1)

NOTE 1 Risk perception reflects the **stakeholder**'s needs, issues and knowledge.

NOTE 2 Risk perception can differ from objective data.

3.3.2.1
external context
external environment in which the organization seeks to achieve its objectives

NOTE External context can include:

— the cultural, 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

— perceptions and values of external **stakeholders**.

3.3.2.2
internal context
internal environment in which the organization seeks to achieve its objectives

NOTE Internal context can include:

— 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);

— internal **stakeholders**;

— policies, objectives, and the strategies that are in place to achieve them;

— perceptions, values and culture;

— standards and reference models adopted by the organization; and

— structures (e.g. governance, roles and accountabilities).

3.3.2.3
risk criteria
terms of reference against which the significance of a **risk** (3.1) is evaluated

NOTE 1 Risk criteria are based on internal and **external context**, and are regularly reviewed to ensure continued relevance.

NOTE 2 Risk criteria can be derived from standards, laws and policies.

3.3.3
risk assessment
overall process of **risk identification** (3.3.4), **risk analysis** (3.3.5) and **risk evaluation** (3.3.6)

3.3.4
risk identification
process of finding, recognizing and describing **risks** (3.1)

NOTE 1 Risk identification involves the identification of **risk sources**, **events** and their causes and their potential **consequences**.

NOTE 2 Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and **stakeholder**'s needs.

3.3.4.1
risk source
anything which alone or in combination has the intrinsic potential to give rise to **risk** (3.1)

NOTE 1 There is no **risk** when another object, person or organization does not have an interaction with a risk source.

NOTE 2 A risk source can be tangible or intangible.

3.3.4.2
event
occurrence or change of a particular set of circumstances

NOTE 1 Nature, **likelihood**, and **consequence** of an **event** can not be fully knowable.

NOTE 2 An event can be one or more occurrences, and can have several causes.

NOTE 3 **Likelihood** associated with the event can be determined.

NOTE 4 An event can consist of a non occurrence of one or more circumstances.

NOTE 5 An event with a **consequence** is sometimes referred to as “incident”.

NOTE 6 An event where no loss occurs may also be referred to as a "near miss", "near hit", "close call" or "dangerous occurrence".

3.3.4.3
hazard
potential source of harm

NOTE Hazard can be a source of **risk**.

3.3.4.4
risk owner
person or entity with the accountability and authority for managing the **risk** (3.1) and any associated **risk treatments** (3.3.7)

3.3.5
risk analysis
process to comprehend the nature of **risk** (3.1) and to determine the **level of risk** (3.3.5.10)

NOTE Risk analysis provides the basis for **risk evaluation** and decisions about **risk treatment**.

3.3.5.1
uncertainty
state, even partial, of deficiency of information related to or understanding or knowledge of an **event** (3.3.4.2), its **consequence** (3.3.5.3), or **likelihood** (3.3.5.2)

3.3.5.2
likelihood
chance of something happening

NOTE 1 This Guide uses the word "likelihood" to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, and described using general terms or mathematically (such as a **probability** or a **frequency** over a given time period).

NOTE 2 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. This Guide therefore uses “likelihood“, with the intent that it should have the same broad interpretation as the term “**probability**“ has in many languages other than English.

3.3.5.2.1
exposure
extent to which an organization is subject to an **event** (3.3.4.2)

3.3.5.3
consequence
outcome of an **event** (3.3.4.2) affecting objectives

NOTE 1 An **event** can lead to a range of **consequences**.

NOTE 2 A consequence can be certain or uncertain and can have positive or negative effects on objectives.

NOTE 3 Consequences can be expressed qualitatively or quantitatively.

3.3.5.4
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 See Note 2 to 3.3.5.2.

3.3.5.5
frequency
measure of the **likelihood** (3.3.5.2) of an **event** (3.3.4.2) expressed as a number of **events** (3.3.4.2) or outcomes per defined unit of time

3.3.5.6
resilience
capacity to resist being affected by an **event** (3.3.4.2)

3.3.5.7
vulnerability
intrinsic properties of something that create susceptibility to a source of **risk** (3.1) that can lead to a **consequence** (3.3.5.3)

3.3.5.8
risk matrix
tool for ranking and displaying **risks** (3.1) by defining ranges for **consequence** (3.3.5.3) and **likelihood** (3.3.5.2)

3.3.5.9
control
measure to modify **risk** (3.1)

NOTE 1 Controls are the result of **risk treatment**.

NOTE 2 Controls include any process, policy, device, practice, or other actions designed to modify **risk**.

3.3.5.10
level of risk
magnitude of a **risk** (3.1) expressed in terms of the combination of **consequences** (3.3.5.3) and their **likelihood** (3.3.5.2)

3.3.6
risk evaluation
process of comparing the results of **risk analysis** (3.3.5) against **risk criteria** (3.3.2.3) to determine whether the **level of risk** (3.3.5.10) is acceptable or tolerable

NOTE Risk evaluation assists in the decision about **risk treatment**.

3.3.6.1
risk attitude
organization's approach to assess and eventually pursue, take or refuse **risk** (3.1)

3.3.6.2
risk appetite
amount and type of **risk** (3.1) an organization is prepared to pursue or take

3.3.6.3
risk tolerance
organization's readiness to bear the **risk** (3.1) after **risk treatments** (3.3.7) in order to achieve its objectives

NOTE Risk tolerance can be limited by legal or regulatory requirements.

3.3.6.4
risk aversion
attitude to turn away from **risk** (3.1)

3.3.6.5
risk aggregation
process to combine individual **risks** (3.1) to obtain a more complete understanding of **risk** (3.1)

3.3.7
risk treatment
process of developing, selecting and implementing **controls** (3.3.5.9)

NOTE 1 Risk treatment can involve:

— avoiding the **risk** by deciding not to start or continue with the activity that gives rise to the **risk**;

— seeking an opportunity by deciding to start or continue with an activity likely to create or enhance the **risk**;

— removing the source of the **risk**;

— changing the nature and magnitude of **likelihood**;

— changing the **consequences**;

— sharing the **risk** with another party or parties; and

— retaining the **risk** by choice.

NOTE 2 Risk treatments that deal with negative **consequences** are sometimes referred to as **risk mitigation**, risk elimination, risk prevention, risk reduction, risk repression and risk correction.

3.3.7.1
risk acceptance
informed decision to take a particular **risk** (3.1)

NOTE 1 Risk acceptance can occur without **risk treatment** or during the process of **risk treatment**.

NOTE 2 Risk acceptance can also be a process.

NOTE 3 **Risks** accepted are subject to **monitoring** and **review**.

3.3.7.2
risk avoidance
decision not to be involved in, or to withdraw from, an activity based on the **level of risk** (3.3.5.10)

NOTE Risk avoidance can be based on the result of **risk evaluation** and/or legal obligations.

3.3.7.3
risk sharing
form of **risk treatments** (3.3.7) involving the agreed distribution of **risk** (3.1) with other parties

NOTE 1 Legal or regulatory requirements can limit, prohibit or mandate **risk sharing**.

NOTE 2 Risk sharing can be carried out through insurance or other forms of contract.

NOTE 3 Risk sharing can create new **risks** or modify existing **risks**.

3.3.7.4
risk financing
form of **risk treatments** (3.3.7) involving contingent arrangements for the provision of funds to meet the financial **consequences** (3.3.5.3) should they occur

3.3.7.5
risk retention
acceptance of the benefit of gain, or burden of loss, from a particular **risk** (3.1)

NOTE 1 Risk retention includes the acceptance of **residual risks**.

NOTE 2 The **level of risk** retained may depend on **risk criteria**.

3.3.7.6
risk mitigation
measures taken to reduce an undesired **consequence** (3.3.5.3)

3.3.7.7
residual risk
risk (3.1) remaining after **risk treatments** (3.3.7)

NOTE 1 Residual risk can contain unidentified **risk**.

NOTE 2 Residual risk is also known as retained **risk**.

3.3.8.1
monitoring
continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected

NOTE Monitoring can be applied to a **risk management framework**, **risk management process** or a **risk**.

3.3.8.2
review
activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives

NOTE Review can be applied to a **risk management framework**, **risk management process** or a **risk**.

3.3.8.3
risk reporting
form of communication intended to address particular internal or external **stakeholders** (3.3.1.1) to provide information regarding the current state of **risk** (3.1) and its management

3.3.8.3.1
risk register
record of information about identified **risks** (3.1)

NOTE The term risk log is sometimes used instead of risk register.

3.3.8.3.2
risk profile
description of a set of **risks** (3.1)

NOTE The set of **risks** can contain those that relate to the whole organization, part of the organization, or as otherwise defined.

3.3.8.4
risk management audit
systematic, independent and documented process for obtaining evidence and evaluating it objectively to determine the extent to which the **risk management framework** (3.2.1) is adequate and effective

Alphabetical index

Bibliography

[1] ISO 704:2000, *Terminology work — Principles and methods*

[2] ISO 860:1996, *Terminology work — Harmonization of concepts and terms*

[3] ISO 3534-1:1993, *Statistics — Vocabulary and symbols — Part 1: Probability and general statistical terms*

[4] ISO 9000:2005, *Quality management systems — Fundamentals and vocabulary*

[5] ISO 10241:1992, *International terminology standards — Preparation and layout*

[6] ISO/IEC Guide 2:2004, *Standardization and related activities — General vocabulary*

[7] ISO/IEC Guide 51:1999, *Safety aspects — Guidelines for their inclusion in standards*