	ISO/TMB/WG Risk Management Secretariat of ISO TMB WG on Risk Management E-mail: risk-management@jsa.or.jp
Doc. ISO/TMB/RMWG	N 48
Date: 2007-06-15	

Title:	Committee Draft of ISO/IEC Guide 73 "Risk management — Vocabulary"
Source:	ISO TMB WG on Risk Management Secretariat
TO	Member bodies and liaison organizations that sent experts to the WG on Risk Management Circulated for comment
CC	Experts
	Comments will be accepted through 15th September, 2007. **Comments received after 15th September, 2007 will not be circulated or considered** in the 5th meeting. Please send comments by E-mail to risk-management@jsa.or.jp. To submit comments, please follow the instructions given in N 49. Explanations on the highlighted part of this document are also given in N49.
Supersedes document:	N30 Working Draft 3 of Guide 73
Medium:	ISO/Livelink www.iso.org/rm, folder "03.Projects", under Sub-folder "N048 2007-06-15 to 2007-09-15 Circulation of Committee Draft of Guide 73"

COMMITTEE DRAFT ISO/IEC CD Guide 73	
Date 2007-06-15	Reference number **ISO/TMB WG on Risk management** **N 48**
Supersedes document N30	

WARNING: This document is not an 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.

ISO/TMB WG on Risk management Secretariat **JISC**	Circulated to member bodies that sent experts to this WG and organizations in liaison for: ☒ discussion at **China** on **2007-12-03 to 12-07** [venue/date of meeting] ☒ comments by **2007-09-15** [date] ☐ approval for registration as a DIS in accordance with 2.5.6 of part 1 of the ISO/IEC Directives, by [date] (members vote only: ballot form attached) **P-members of the technical committee or subcommittee concerned have an obligation to vote.**

English title

Risk management — Vocabulary

French title

Reference language version: ☒ English ☐ French ☐ Russian

Introductory note

ISO/TMB WG on Risk management N 048

Date: 2007-06-15

ISO/IEC CD Guide 73

ISO/TMB WG on Risk management

Secretariat: JISC

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: International Standard
Document subtype:
Document stage: (30) Committee
Document language:E

16 # Contents

Page

27

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.

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

The main task of technical committees is to prepare International Standards. Draft Guides adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member 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 shall not be held responsible for identifying any or all such patent rights.

The first edition of ISO/IEC Guide 73 was prepared by the ISO Technical Management Board Working Group on risk management terminology. The 2nd edition has been developed by the ISO TMB WG on risk management in association with the development of ISO 31000 to reflect changes in risk management practices and feedback from users.

This Guide may be revised after 5 years on the basis of practical experience. Committees writing standards are invited to inform the ISO Central Secretariat of any difficulties encountered with the implementation of its provisions.

Introduction

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

These objectives may relate to a range of the organization's activities, from strategic initiatives to its operations, processes and projects, and be reflected in terms of societal, environmental, safety and security outcomes, commercial, financial and economic measures, as well as social, cultural, political and reputation impacts.

All activities of an organization involve risks that must be managed. The risk management process aids decision making by taking account of uncertainty and the possibility of future events or circumstances (intended or unintended) and their effects on agreed objectives.

Risk management involves applying logical and systematic methods for:

— communicating and consulting throughout this process;

— establishing the organization’s context for identifying, analysing, evaluating, treating, and monitoring risk associated with any activity, product, function or process; and

— reporting the results appropriately.

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

Risk management — Vocabulary

1 Scope

This Guide provides a basic vocabulary of the definitions of risk management generic terms. 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 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 guidelines on the implementation of risk management, reference should be made to ISO 31000.

NOTE The term “standard” — used throughout this Guide — includes Technical Reports and Guides, as well as to International Standards, and other related publications dealing with some aspect of risk management. Such standards can deal exclusively with the management of risk or can include clauses specific to the management of risk.

2 Overview of risk management terms and definitions

The relationships among the terms and definitions for risk management are shown in Figures 1 and 2.

Risk management depends on the context in which it is used. The words used in each context may vary. In some cases it may be necessary to deviate from the exact wording offered in this Guide to meet the needs of a specific domain. In this case, care should be taken to ensure that terminology actually used does not conflict with this Guide and that the rationale for any deviation should be made clear.

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. Accordingly, this Guide provides definitions for the various meanings that each term is likely to have, without giving definitions that contradict each other.

In addition to managing threats to their objectives, organizations are increasingly applying risk management processes in order to optimize 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 the whole risk spectrum.

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.

3 Terms and definitions

3.1 Basic Terms

3.1.1
risk
effect of **uncertainty** (3.1.17) on objectives

NOTE 1 An effect may be positive, negative, or a deviation from the expected.

NOTE 2 An objective may be financial, related to health and safety, or defined in other terms.

NOTE 3 Risk is often described by an event, a change in circumstances, a consequence, or a combination of these and how they may affect the achievement of objectives.

NOTE 4 Risk can be expressed in terms of a combination of the consequences of an event or a change in circumstances, and their likelihood.

3.1.2
consequence
outcome of an **event** (3.1.4) or change in circumstances affecting the achievement of objectives

NOTE 1 An **event** or a particular change of circumstances may lead to a range of **consequences**.

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

3.1.3
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 estimated objectively or subjectively, or in terms of general descriptors (such as rare, unlikely, likely, almost certain), frequencies or (mathematical) probabilities.

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.

3.1.4
event
occurrence or existence of a particular set of circumstances

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

NOTE 2 An event can be a single occurrence or a series of occurrences.

NOTE 3 Likelihood associated with the event can be estimated.

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

NOTE 5 Sometimes an unpredictable event is called “incident”.

3.1.5
incident
event (3.1.4) in which a loss occurred or could have occurred regardless of **severity** (3.3.7)

NOTE An **event** where no death, ill health, injury, damage or other loss occurs may also be referred to as a "near-miss", "near-hit", "close call" or "dangerous occurrence".

3.1.6
exposure
susceptibility to gain or loss, usually quantified in terms of potential impact

NOTE 1 An **exposure** is a **risk** with any **likelihood** of occurrence.

NOTE 2 In financial sectors, the **likelihood** of the **exposure** is often assumed to be the total loss of an asset or production process.

NOTE 3 "**Vulnerability**" has a similar meaning as **exposure** but is usually only applied to loss.

3.1.7
risk criteria
terms of reference against which the significance of a **risk** (3.1.1) is evaluated

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

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

3.1.8
level of risk
magnitude of a **risk** (3.1.1) measured in terms of the combination of **consequences** (3.1.2) and their **likelihood** (3.1.3)

3.1.9
risk tolerability
level of risk (3.1.8) which an organization will tolerate

3.1.10
risk management
coordinated activities to direct and control an organization with regard to **risk** (3.1.1)

3.1.11
risk management plan
decision on approach and plan for the management of **risk** (3.1.1) throughout the organization

3.1.12
risk management process
systematic application of management policies, procedures and practices to the tasks of communicating, consulting, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing **risk** (3.1.1)

3.1.13
risk management policy
overall intentions and direction of an organization related to the management of **risk** (3.1.1) as formally approved by top management

3.1.14
risk management framework
set of interrelated activities and rules for coordinating and directing **risk management processes** (3.1.12) within an organization

NOTE 1 The **risk management framework** should be integrated with the organization's overall strategic, tactical and operational policies and practices.

NOTE 2 The **risk management framework** sets the context in which **risks** are identified, assessed, treated, monitored and reviewed.

3.1.15
risk management system
management system to direct and control and organization with regard to **risk** (3.1.1)

NOTE 1 **Risk management system** elements include strategic planning, decision making, organizational structure, responsibilities, practices, processes, procedures and resources for dealing with **risks**.

NOTE 2 The culture of an organization is reflected in its **risk management system**.

NOTE 3 The **risk management system** should be part of and integrated within the organization's overall management system.

3.1.16
risk source
object or activity which may cause a **risk** (3.1.1)

NOTE 1 There is no **risk** (3.1.1) when another object, person or organization does not have an interaction with a **risk source**.

NOTE 2 A **risk source** might be tangible or intangible.

3.1.17
uncertainty
state, even partial, of deficiency of information related to a future **event** (3.1.4), **consequence** (3.1.2), or **likelihood** (3.1.3)

3.2 Terms related to people or organization affected by risk

3.2.1
external context
any elements outside the organization that influence objectives

NOTE **External context** may include:

— cultural, political, legal, regulatory, financial, economic and competitive environment, whether international, national or regional;

— key drivers and trends having impact on the objectives of the organization; and

— perceptions and values of external stakeholders.

3.2.2
internal context
any elements within the organization that influence the way in which an organization manages **risk** (3.1.1)

NOTE **Internal context** may include:

— capabilities, understood in terms of resources and knowledge (e.g. capital, people, competencies, processes, systems and technologies);

— information flows and decision making processes;

— internal **stakeholders**;

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

— perceptions, values and culture;

— policies and processes;

— standards and reference models adopted by the organization; and

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

3.2.3
risk management context
process of identifying information that may have an influence on the management of **risk** (3.1.1) (goals, objectives, strategies, scope and parameters)

3.2.4
risk communication and consultation
continuous or iterative process that an organization conducts to provide, share and obtain information and to engage in dialogue with **stakeholders** (3.2.5) regarding the management of **risk** (3.1.1)

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

NOTE 2 The **risk** communication process includes specific activities of consultation with **stakeholders**.

NOTE 3 The **risk** communication can be internal or external.

NOTE 4 The internal communication may be in the form of a report as a support for decision making.

3.2.5
stakeholder
person or group concerned with, affected by, or perceiving themselves to be affected by an organization

NOTE 1 A decision maker is also a **stakeholder**.

NOTE 2 The term "**stakeholder**" includes but has a broader meaning than "interested party".

3.2.6
risk perception
stakeholder 's (3.2.5) view on a **risk** (3.1.1)

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

NOTE 2 **Risk perception** can differ from objective data.

3.2.7
risk owner
person with the authority and accountability to make a decision to treat, or not to treat a **risk** (3.1.1)

NOTE Anyone who has accountability for an objective also has accountability for the **risks** associated with the objective and controls to manage those **risks**.

3.3 Terms related to risk assessment

3.3.1
risk assessment
overall process of **risk identification** (3.3.2), **risk analysis** (3.3.3) and **risk evaluation** (3.3.12)

3.3.2
risk identification
process of finding, recognizing and describing **risks** (3.1.1)

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

NOTE 2 The identification may include historical data, theoretical analysis, informed opinions and the **stakeholders** needs.

3.3.3
risk analysis
systematic process to comprehend the nature of **risk** (3.1.1) and to deduce the **level of risk** (3.1.8)

NOTE 1 **Risk analysis** provides the basis for **risk evaluation** and decisions about **risk treatment**.

NOTE 2 Information can include, but is not limited to, available experiences, theoretical assumptions, informed opinions, and the views of **stakeholders**.

3.3.4
absolute risk
level of risk (3.1.8) without taking into account existing **risk controls** (3.4.2)

3.3.5
probability
measure of the chance of occurrence expressed as a number between 0 and 1, where 0 is impossibility and 1 is absolute certainty

3.3.6
frequency
number of occurrences of an **event** (3.1.4) or outcome per defined period of time

3.3.7
severity
extent of a loss, harm or damage

3.3.8
risk estimation
process used to assign values to **consequences** (3.1.2), their **likelihood** (3.1.3) and to the **level of risk** (3.1.8)

NOTE 1 **Risk estimation** can consider cost, benefits, the concerns of **stakeholders**, and other variables as appropriate for **risk evaluation**.

NOTE 2 The **risk estimation** process can be carried out by making use of both quantitative and qualitative procedures.

3.3.9
risk rating
categorization of **risks** (3.1.1) based on the **level of risk** (3.1.8)

3.3.10
risk appetite
amount and type of **risk** (3.1.1) an organization is prepared to pursue or take

NOTE **Risk appetite** is a reflection of how an organization balances its goals of efficiency, growth, return, and **risk**.

3.3.11
control environment
internal circumstances and conditions that influence the way **risk** (3.1.1) is managed by the organization's employees and provides disciplines and structures as the foundation for all other components of internal control and the management of **risk** (3.1.1)

NOTE **Control environment** factors include the integrity, ethical values, management's operating style, delegation of authority and systems, as well as the processes for managing and developing people in the organization.

3.3.12
risk evaluation
process of comparing the results of the **risk analysis** (3.3.3) against **risk criteria** (3.1.7) to determine the **level of risk** (3.1.8) and whether it is tolerable or not

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

3.3.13
risk matrix
tool for ranking and displaying **risks** (3.1.1) by defining **risk** (3.1.1) categories (e.g. financial **risks** (3.1.1), safety **risks** (3.1.1), environmental **risks** (3.1.1)) and defining ranges for **consequences** (3.1.2) and levels of **likelihood** (3.1.3) for each category

NOTE A **risk matrix** should also indicate the organization's acceptability of certain **risks**.

3.3.14
risk profile
description of an organization’s **risk** (3.1.1)

NOTE 1 This may take the form of a collection of **likelihood**/**probability** pairs usually in order of **level of risk**.

NOTE 2 In some cases, a **risk profile** may be expressed as a **likelihood**/**probability** distribution of **consequences**.

3.3.15
risk tolerance
organization’s readiness to accept a **residual risk** (3.4.17) after **risk treatment** (3.4.1) in order to achieve the organization’s objectives

3.3.16
vulnerability
a weakness of an asset or group of assets that can be exploited by one or more threats

[ISO/IEC 13335-1:2004]

3.3.17
risk aversion
risk-based policy to evaluate and refuse **risks** (3.1.1)

NOTE **Risk aversion** is the counterweight of **risk appetite**.

3.3.18
heat map
overview of the organization's main **risks** (3.1.1) plotted in its **risk matrix** (3.3.13)

NOTE The **risks** can be plotted as **absolute risks** or as the **residual risks**, when response measures are in place, or as a combination of both.

3.3.19
risk aggregation
process to identify and illustrate the interaction of several, differently correlated individual **risks** (3.1.1) of an organization in order to obtain the overall **risk** (3.1.1)

3.3.20
risk diversification
selection of different **risk** (3.1.1) units in order to reduce potential losses

NOTE In the economic-financial sector, an example of **risk diversification** is the "portfolio diversification".

3.3.21
managed risk
level of risk (3.1.8) taking into account existing **risk controls** (3.4.2)

3.3.22
risk register
document used for recording **risk management process** (3.1.12) for identified **risks** (3.1.1)

NOTE Arranging **risks** in the register linked to objectives converts **risk** information into **risk** knowledge, and facilitates the ownership and management of each **risk**.

3.4 Terms related to risk treatment and control

3.4.1
risk treatment
development and implementation of measures to modify **risk** (3.1.1)

NOTE **Risk treatment** measures may include:

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

b) seeking an opportunity by deciding to start or continue with an activity likely to create or maintain the **risk**;

c) changing the **likelihood**;

d) changing the **consequences**;

e) sharing the **risk** with another party or parties; and

f) retaining the **risk**, either by choice or by default

3.4.2
risk control
measures to modify **risk** (3.1.1)

NOTE 1 **Risk control** may be a result of **risk treatment**.

NOTE 2 **Risk control** includes any process, policy, device, practice, or other actions designed to minimize **risk**.

3.4.3
risk optimization
planning and implementation of measures that act on **likelihood** (3.1.3), impacts and cause in order to minimize losses and to maximize gains

3.4.4
risk prevention
measures taken to reduce the **likelihood** (3.1.3) that an undesired **event** (3.1.4) occurs

3.4.5
risk reduction
combination of **risk prevention** (3.4.4), **risk repression** (3.4.14) and/or **risk mitigation** (3.4.6)

3.4.6
risk mitigation
measures taken to reduce the effect of an undesired **consequence** (3.1.2)

3.4.7
risk sharing
allotting with other parties the benefit of gain or burden of loss for a **risk** (3.1.1)

NOTE 1 Legal or regulatory requirements can limit, prohibit or mandate the transfer of certain **risk**.

NOTE 2 **Risk sharing** can be carried out through insurance or other agreements.

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

3.4.8
risk financing
provision of funds to meet the cost of **risk treatment** (3.4.1) and for the financial **consequences** (3.1.2) of the **risk** (3.1.1) should it occur

NOTE In some industries, **risk financing** refers to funding related only to the financial **consequences** relating to **residual risk**.

3.4.9
risk retention
acceptance of the benefit of gain, or burden of loss, from a particular **risk** (3.1.1)

NOTE 1 **Risk retention** includes the acceptance of **risk**s that have not been identified as well as **residual risks**.

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

3.4.10
risk acceptance
informed decision to take a particular **risk** (3.1.1)

NOTE **Risk**s accepted should be subject to monitoring and review.

3.4.11
acceptable risk
level of **risk reduction** (3.4.5) which is as low as reasonably practicable

3.4.12
ALARP
as low as reasonably practicable

NOTE A concept used for managing **risks** with significant potential health, safety or environmental **consequences** to a level as low as reasonably practicable, but is also applicable for managing other **risks**.

3.4.13
risk elimination
reduction of the **frequency** (3.3.6) of an unfavourable **event** (3.1.4) and/or its **severity** (3.3.7) to zero

NOTE Elimination may involve the removal of hazard(s).

3.4.14
risk repression
measures taken to reduce the **likelihood** (3.1.3) that an undesired **event** (3.1.4) leads to a **consequence** (3.1.2)

3.4.15
risk avoidance
decision not to be involved in, or to withdraw from, an activity based on the **level of risk** (3.1.8) involved

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

3.4.16
risk correction
measures taken to recover from the effect on an undesired **consequence** (3.1.2)

3.4.17
residual risk
risk (3.1.1) remaining after **risk treatment** (3.4.1)

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

NOTE 2 **Residual risk** may also be known as retained **risk**.

3.4.18
risk monitoring
monitoring of **risk management** procedures, particularly **risk treatment** (3.4.1) processes, to assess whether they are effectively implemented and achieving their planned aims

NOTE Where appropriate, **risk monitoring** also includes monitoring the **risk** environment for changes that might affect the **risk management plan**.

3.4.19
risk management review
structured activity undertaken to determine the suitability, adequacy and effectiveness of the **risk management** policies and procedures to achieve established objectives

NOTE 1 **Risk management review** can lead to fine tuning or more substantial changes to **risk management**.

NOTE 2 Many organizations will have regular reviews of their policies and procedures to ensure that they remain fit for purpose.

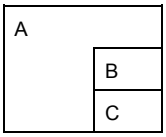
3.4.20
risk reporting
development of reports including strategic, operational, financial and compliance-related **risk** (3.1.1) information, as a basis for directing and controlling the organization as well as for external accounting

NOTE **Risk reporting** should ensure effective communication and information flows of both downwards and upwards throughout the organization as well as to external interested parties such as customers, suppliers, regulators and shareholders.

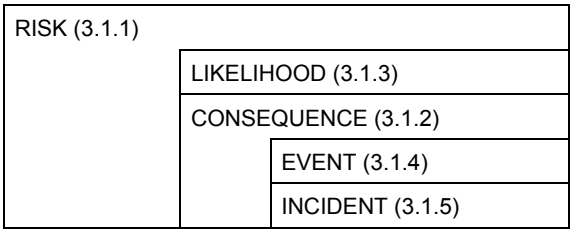
3.4.21
risk audit
systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the **risk management** policies and procedures are fulfilled.

447

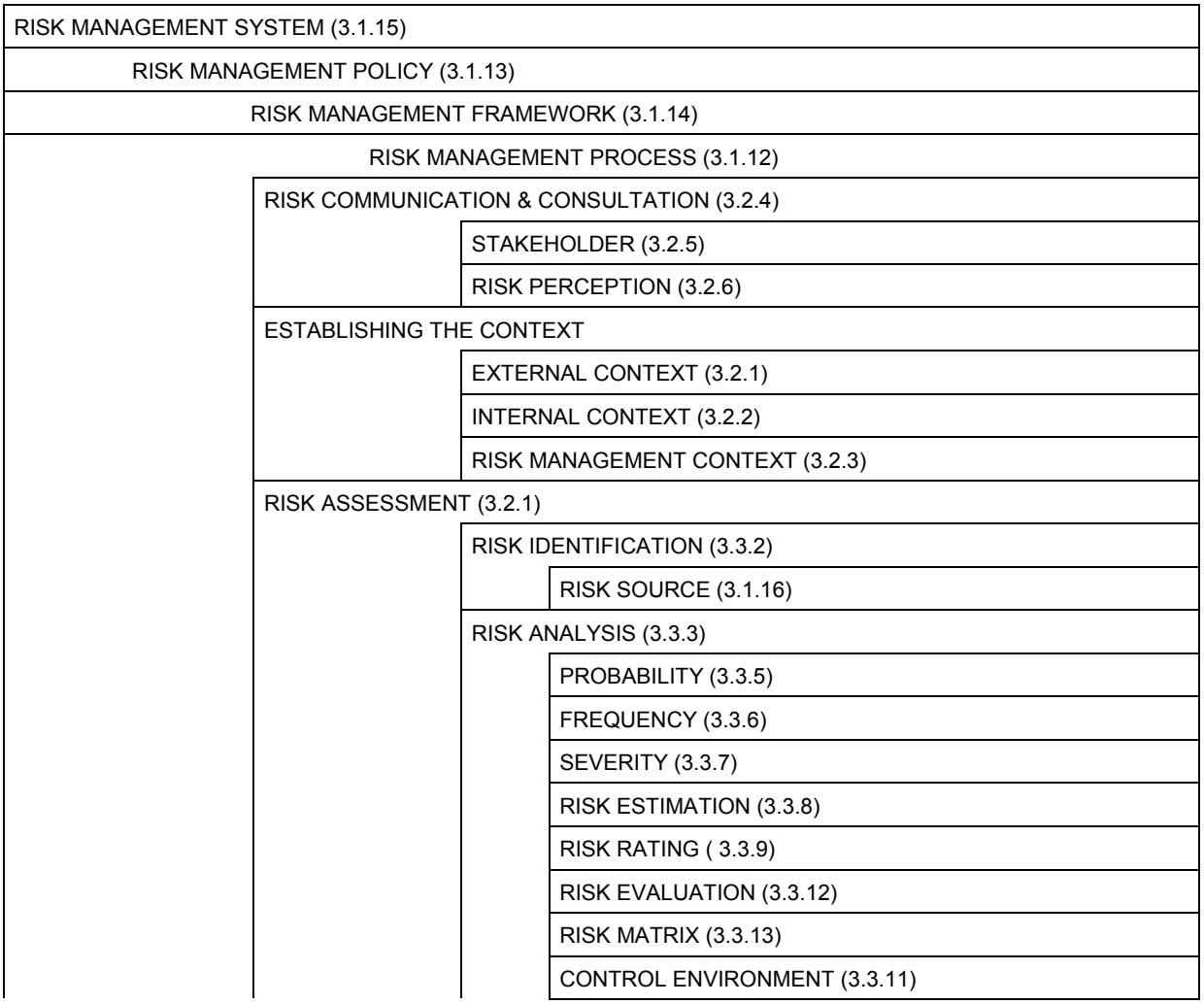
448 Key



449 The terms B and C are used in the definition of the term A or the notes to definition A.
450



451 **Figure 1 — Relationship between terms, based on their definitions regarding "Risk"**



<table>
<tr><td rowspan="11"></td><td rowspan="4"></td><td colspan="2">RISK EVALUATION (3.3.12)</td></tr>
<tr><td rowspan="3"></td><td>RISK APPETITE (3.3.10)</td></tr>
<tr><td>RISK TOLERANCE (3.3.15)</td></tr>
<tr><td>RISK AVERSION (3.3.17)</td></tr>
<tr><td colspan="2">RISK TREATMENT (3.4.1)</td></tr>
<tr><td rowspan="6"></td><td>RISK ACCEPTANCE (3.4.10)</td></tr>
<tr><td>RISK OPTIMIZATION (3.4.3)</td></tr>
<tr><td>RISK SHARING (3.4.7)</td></tr>
<tr><td>RISK RETENTION (3.4.9)</td></tr>
<tr><td>RISK REDUCTION (3.4.5)</td></tr>
<tr><td>RISK AVOIDANCE (3.4.15)</td></tr>
<tr><td colspan="2">RISK MANAGEMENT REVIEW (3.4.19)</td></tr>
<tr><td rowspan="3"></td><td>RISK MONITORING (3.4.18)</td></tr>
<tr><td>RISK REPORTING (3.4.20)</td></tr>
<tr><td>RISK AUDIT (3.4.21)</td></tr>
</table>

452 **Figure 2 — Relationship between terms based on their definitions regarding risk management**

453

453
454
455
456

Alphabetical index

457
458

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] IEC 60050-191:1990, International Electrotechnical Vocabulary — Chapter 191: Dependability and quality of service

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

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