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 71**
Date: 2008-08-27	Supersedes document: None

Title:	Committee Draft 2 of ISO/IEC Guide 73 (N66) with changes proposed in N 70
Diffusion:	ISO/TMB WG on Risk Management Experts
Circulated for:	Use in the Singapore meeting
Note:	This file will be projected on the screen while we discuss comments in the meeting. This is a draft in which all the comments received on CD2 of Guide 73 (N 70) are temporarily added in the original Committee Draft using the "Track Change" function. These files have been prepared for reference and for saving time of typing during the meeting. Please note that we have only TEMPORARILY added ALL the suggested changes in the files. We will edit this file based on the decisions to be made in the meeting. This should progressively provide the meeting with a clean copy of the documents as we proceed through the comments.
Explanation	In this document, the following abbreviations are used. RP = comment proposing replacement, DL = comment proposing deletion of the part New = proposal of new addition to the text
Contents	**Page 1-21:**Text with changes **Page 22-23:** Figure 1 **Page 24:** Proposals of terms to be included in Clause 3 of ISO 31000 **Page 25-27:**List of newly proposed terms
Medium:	ISO/Livelink www.iso.org/rm, folder "03.Projects"

37	37		**Introduction**	
38	38		17Society, its members and its many types of Organizations of all types and sizes 16are exposed to uncertain scenarios and therefore have to face a range of risks that can affect the achievement of their objectives.	
		15	Organizations of all types and sizes face a range of risks when trying to achieve their objectives.	
39	41		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 19, regulatory and reputational outcomes and impacts.	
42	43		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.	
44	44		21The Risk management process involves applying logical and systematic methods for:	
		20	Either (alternative 1) extend the scope of the standard to all kind of risk management process (including land use planing for natural risks) and come back to the basic definition of risk, as the combination of likelihood and consequences, without relation with objectives achievement, Or (alternative 2 - preferred alternative) specify in the introduction that the document aims at providing a vocabulary to organizations of any kind for the management of the risks these organizations are exposed.	
45	45		— communication and consultation throughout the process;	
46	46		— establishing the context;	
47	48		— identifying, analyzing, evaluating 22 prioritizing and treating risk associated with any activity, process, function, project, product, service 24 objectives or asset;	
49	49		— monitoring and reviewing risk; and	
50	50		— recording and reporting the results appropriately.	

51	52		This Guide provides a basic vocabulary to develop common understanding on risk management 27 and related concepts and terms among 26standard developers and standard users [organizations 28/functions and across different applications and types of risk management functions.]	
53	53		This Guide is generic and is compiled to encompass the general field of risk management.	
54	54		When using risk management terminology, the definitions in this Guide should be given first consideration.	
		29	Other definitions and uses of the terms in Guide 73 do exist and may conflict with the definitions given herein. Effectively managing risks requires clear communications about risks to an organization, industry, sector and stakeholders. Common understanding of terms is necessary for clear communications. In the long term, developing a common set of terms is desired in the international community. In the near term, organizations or industries that have a common understanding of risk management terms using definitions that conflict with those in this Guide 73 may choose to continue using the differing definitions to facilitate effective communications within that organization or industry.	
55	55		**Risk management — Vocabulary 83— Guideline for use in standards**	
56	56		**1 Scope**	
57	60		This Guide provides the definitions of generic terms related to risk management. ~~This Guide~~30It aims to encourage a mutual and consistent understanding 31 of and, a coherent approach to the description of activities relating to the 32standardization of management of risk, and use of uniform risk management terminology in 32processes and frameworks standards dealing with the management of risk.	
		RP33	This Guide is intended to be used by those engaged in managing risks, for example developers of national or sector specific standards, guides, procedures and codes of practice relating to the management of risk.	
61	61		This Guide is intended to be used by:	
62	62	**32 DL**	— those engaged in managing risks 34in practice;	3

63	63		— those who are involved in activities of ISO and IEC; and	1
64	65		— developers of national or sector specific standards, guides, procedures and codes of practice relating to the management of risk.	2
66	66		For principles and guidelines on the implementation of risk management, reference is made to=>36 See ISO 31000.	
		37	ISO/IEC Guide 51 applies for safety related aspects.	
67	67		**2 Overview of risk management terms and definitions**	
68	71		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.	
		38	Thus, certain applications may use different or even conflicting definitions of terms defined in this Guide 73.	
72	74		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.	
74	77		The terms and definitions in this Guide 39 which is confined to management and evaluation of risks 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 40intrinsic undesirable (negative) consequences. Since organizations increasingly adopt a broader approach to the management of risk, this Guide addresses all applications and sectors.	
78	78		The relationship between the terms for risk management is shown in Figures 1.	
79	80		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	81			
82	82		**Figure 1 — Relationship between terms based on their definitions regarding risk management**	
			3 Terms and definitions	
			3.1 risk	
			Effect91=>resultant of **uncertainty** (3.3.5.1) 89 or randome events on 92 achieving objectives	
		90	combination of likelihood and consequences of an hazardous event	
		91	Potential set of events subject to uncertainty and their related consequences on objectives	
			NOTE 1 An effect is 92=> Uncertainty can lead to a deviation from the expected - positive 93DLand/or negative.	
		96	NOTE 1 An effect may be positive, negative, or a deviation from the expected.	
			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 98DLan **event** or a change in circumstances, and the associated **likelihood** of occurrence 99 of those consequences.	
		94	NOTE 5 Each sector should do an interpretation of this definition of risk according to its context, requirements and needs.	
		226	NOTE 6 Uncertainty is 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)	
			3.2 risk management	
			coordinated activities, 100 procedures and resources to direct and control an organization with regard to **risk**	

			(3.1)102=>adverse risk events.	
		101	activities to understand and if appropriate treat risk	
			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 104 risk management and **risk management 103DLprocesses** (3.3) throughout the organization	
			NOTE 1 The foundations 103 may include the policy, objectives, mandate and commitment to manage **risk**.	
			NOTE 2 The organizational arrangements include plans, relationships, accountabilities, resources, 105projects, processes and activities.	
			NOTE 3 The risk management framework is 103 generally embedded within the organization's overall strategic and operational policies and practices.	
		103	NOTE 4 The risk management framework can be applied to a particular product, process and project, and part or whole of the organization.	
			3.2.2 risk management policy	
			107 expression of , 108 documented statement of the overall intentions and direction =>106 guidelines of an organization related to **risk management** (3.2)	
			3.2.3 risk management plan	
			document => 109 series of scheme and arrangement 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 112 chronological sequence 111 and timing 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	
			114&116systematic 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)	
			3.3.1 119&120 risk communication and consultation	
			continual or=>117 and iterative processes that an organization conducts to provide, share or obtain information and to ~~engage~~ participate in dialogue with **stakeholders** (3.3.1.1) 128 or others regarding the management of **risk** (3.1)=>119 risk management	
			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 122 two way process of informed communication between organization and its **stakeholders** 128 or others on an issue prior to making a decision or determining a direction on a particular issue. Consultation is:	
			— a process not an outcome 123DIwhich impacts on a decision through influence rather than power; and	
			— 124 an input about inputs to decision making, not joint decision making.	
			NOTE 3 130DLInternal 132 and external communication and consultation should be appropriately recorded.	
			3.3.1.1 stakeholder	
			any person or organization that can affect, be affected by, or perceive 135?themselves to be affected by a decision or activity 136 of another entity/organization	
		139	that can affect or be affected by a decision or activity. Potential stakeholders include any person or organization	

			that perceives themselves to be affected by a decision or activity.	
			NOTE A decision maker is also a stakeholder. 140=> can also be a stakeholder.	
		141DL	**3.3.1.2 risk perception=>144 perception of risk**	
			stakeholder's (3.3.1.1) view on a **risk** (3.1)	
		142	subjective interpretation of risk	
		143	#1. Risk perception is subjective and can differ from objective data. #2. Risk perception includes subjective values and beliefs which must be considered in consultation.	
			NOTE 1 Risk perception=>144 Perception of risk reflects the **stakeholder**'s needs 144 preferences, issues and knowledge 145 beliefs and values.	
		146DL	NOTE 2 Risk perception can differ from objective data.	
		147NEW	**establishing the context** Processes that an organization conducts to build the interrelated conditions in which it exists regarding the management of risk (3.1). NOTE1 The interrelated conditions can include internal factors and external factors of an organization which can impacts on its actors of management risk. NOTE2 The context of an organization can't be build in one day, it need emend and perfect continually and iteratively.	
		148NEW	**risk contextualization** identification of the parameters within which the risk (3.1.13) is to be managed, and of risk criteria (3.3.4).	
		150NEW	**3.3.2. establishing the context** establishing the environment in which the organization seeks to achieve its objectives	
		151 RP	**external factors**	

			the elements of the environment, not managed by the organization, in which the organization seeks to achieve its objectives. Note: The external factors are by definition, not managed by the organization	
			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, 153 social financial, technological, economic, natural 149. social and competitive environment, whether international, national, regional or local 154 or social community;	
			— key drivers and trends having impact on the objectives of the organization; and	
			— **155 risk perceptions** and values of external **stakeholders** 152 and their risk appetite.	
		156NEW	**internal factors** elements of the environment, managed by the organization, in which the organization seeks to achieve its objectives. Note: The internal factors are by definition, managed by the organization.	
			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**; =>157 internal stakholders perceptions and value	
			— policies, objectives, and the strategies that are in place to achieve them;	
			— **158risk perceptions**, values and culture;=>157 organizational culture	
		159RP	— Perception and values of internal stakholders	

			— standards and reference models adopted by the organization; and	
			— structures (e.g. governance, roles and accountabilities) 157 and their risk appetite.	
		160	— perceptions and values of internal stakeholders and the organization's culture	
			3.3.2.3 risk criteria	
			terms of reference against which the significance of a **risk** (3.1) is evaluated=>161 compared	
		162RP	terms of reference established according to the organization's objectives and to the context	
			NOTE 1 Risk criteria are based on **internal =>Check with ISO/CS editor** and **external context [DL 165**, and are=>164 need to be regularly reviewed to ensure continued relevance.**]**	
		168RP	Risk criteria are based on the organizational objectives and reflect the internal and external environment	
		169DL	NOTE 2 Risk criteria can be derived from standards, laws and policies 170 and other requirements.	
			3.3.3 risk assessment	
			overall process of **risk identification** (3.3.4), **risk analysis** (3.3.5) and **risk evaluation** (3.3.6) 172 and level or overall system risk (See related proposal in comment No.411)	
		173NEW	**Suggestion 1: examples of footnotes that could be added at the appropriate locations** "Risk assessment" here includes "Risk assessment" and the first step of "Risk management" according to the Codex Alimentarius Commission (CAC) and the World Organization for Animal Health (OIE). "Risk analysis" here corresponds only to the process leading to the "Risk characterization". Yet "risk characterization" is the last component of "risk assessment" according to the Codex Alimentarius Commission (CAC) and the World Organization for Animal Health (OIE). The later process and "risk communication" as well do not belong to the "risk management" according to the Codex Alimentarius Commission (CAC) and the World Organization for Animal Health (OIE). "Risk analysis" according to the Codex Alimentarius Commission (CAC) and the World Organization for Animal	

			Health (OIE) has three components: (1) "risk assessment" (composed of "risk identification", "hazard assessment", "exposure assessment" and "risk characterization"), (2) "risk management" and (3) "risk communication". **Alternative suggestion 2: limiting the field of application** In Section 1, please indicate: "This Guide is not intended to be used by those engaged if managing risk for food safety or animal health. Documents published by the Codex Alimentarius Commission (CAC) and the World Organization for Animal Health (OIE) apply in these fields."	
			3.3.4 risk identification	
			process of finding, recognizing and describing **risks** (3.1)	
			combination of the probability of an event and its consequence.	
			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.	
		176DL	**3.3.4.1 risk source**	
			anything which alone or in combination has the intrinsic potential to give rise to **risk** (3.1) 177 at decline control measure situation	
		178-181	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 75 risk event	

			occurrence or change of a particular set of circumstances	
		185DL	NOTE 1 Nature, **likelihood**, and **consequence** of an **event** can not be fully knowable=>188 fully known or fully determined.	
			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=>192 estimated.	
			NOTE 4 An event can consist of a non occurrence of one or more circumstances.	
			NOTE 5 An event DL198 [with a 195&197 negative **consequence]** is sometimes referred to as "incident" 197 or accident depending on the damages caused..	
		196RP	NOTE 5 An event may be called an incident depending on the consequences.	
			NOTE 6 An event where no loss occurs 202 but could have occurred may also be referred to as a "near miss", 201"incident",""near hit", "close call" or "dangerous occurrence".	
		204NEW	**Level of risk** is expressed in terms of consequences and their likelihood. This often will not be just the likelihood of the preceding event that could give rise to the consequences.	
		205NEW	Note XX The likelihood of a particular set of consequences being experienced will not necessarily be the same as the likelihood of the underlying event(s) which gave rise to those consequences. The level of Risk is measured in terms of the likelihood of the consequences, not of the event that gave rise to the consequences.	
			3.3.4.3 hazard	
			[206 DIpotential] source of harm	
		208RP	cause or source of potential damage or loss	
			NOTE Hazard can be a ~~source of risk~~**212risk source**.	
			3.3.4.4 risk owner	

			person or entity with the accountability and authority ~~for managing the **risk** (3.1)~~ 216DL[to manage risk and any associated **risk treatments** (3.3.7)] 218 and subsequent adverse or positive risk	
			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**.	
		220	NOTE 2 Risk analysis is sometimes called risk estimation.	
			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)	
		223	Existence of multiple future events that have outcome affecting objectives	
		224	state, even partial, of deficiency of information, understanding or knowledge.	
		228	state in which an event, its consequence, or likelihood cannot be assertively determined.	
		231	State of deficiency of information related to an event	
			3.3.5.2 likelihood	
			chance of something happening	
		234	Used as a general description of probability or frequency. NOTE Can be expressed qualitatively or quantitavely.	
			NOTE 1 This Guide uses the word "likelihood" to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively =>235 qualitatively or quantitavely, 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 247 meaning the measure of the chance of occurrence expressed as a number between 0 and 1, where 0 is impossibility and 1 is absolute certainty. 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=>239 risk to which an 236 asset, project, entity or 240 a person or organization is subject to an **event** (3.3.4.2)	
			3.3.5.3 consequence	
			outcome of an **event** (3.3.4.2) 242&243 DL[affecting objectives]	
		243RP	Consequence Outcome or impact of an event (1.3.4) NOTE 1: There can be more than one consequence from one event. NOTE 2: Consequences can range from positive to negative. NOTE 3: Consequences can be expressed qualitatively or quantitatively. NOTE 4: Consequences are considered in relation to the achievement of 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 245DL[on objectives.] 246 each with its respective likelihood **246** NOTE XX Initial consequences may escalate through knock-on effects NOTE YY The Consequences of one event may become an event in relation to a different set of objectives (and	

			therefore, risks). NOTE ZZ A Consequence may be the result of several events	
			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, 248 NOTE where 0 is impossibility and 1 is absolute certainty	
			NOTE See Note 2 to 3.3.5.2.	
		249NEW	For planning purposes, the probability of occurrence may be set to "1" when its necessary to plan for a scenario where the assumption is that the incident will occur.	
			3.3.5.5 frequency	
			measure of the **likelihood** (3.3.5.2)=>250 probability 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)	
		251RP	capacity to cope with and event	
		252RP	Capacity to recover in time from being affected by an event	
		253 RP	Capacity to achieve its objective being affected by an event	
			3.3.5.7 vulnerability	
			intrinsic properties of something 256DL[that create susceptibility to a ~~source of~~ **risk** source (257&258) (3.1) that can lead to a **consequence** (3.3.5.3)]	
		255 RP	Intrinsic properties of something to be affective by a ~~source of~~ risk source (257&258)	
			3.3.5.8 risk 263 prriority matrix	

			tool for ranking and displaying **risks** (3.1) by defining ranges for **consequence** (3.3.5.3) and **likelihood** (3.3.5.2)	
		262RP	tool for ranking and displaying **risks** (3.1) according to risk criteria	
		261RP	tool for ranking and displaying risks according to their consequence and likelihood of occurrence	
		264NEW	NOTE: *add examples*	
			3.3.5.9 75&268&269&271 risk control	
			measure to modify **risk** (3.1)	
		272	measure that is modifying risk	
		266RP	steps taken to maintain or modify the level of risk	
		270RP	activity to implement risk treatmen	
			NOTE 1 Controls are the result of **risk treatment**.	
		274	NOTE 1 Risk treatments once implemented become or modify controls	
			NOTE 2 Controls include any process, policy, device, practice, or other actions designed to=>274 which modify **risk**.	
		272NEW	NOTE 3 Most controls have a degree of inherent unreliability and consequently may not always exert the intended or assumed modifying effect	
		267RP	existing process, policy, device, practice or other action that acts to minimize negative risks or enhance positive opportunities. NOTE The word 'control' may also be applied to a process designed to provide reasonable assurance regarding the achievement of objectives.	
			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) 276=>risk criteria	

		278NEW	NOTE Normally the level of risk will be presented in a risk matrix.	
			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 DL279**level of risk** (3.3.5.10) is acceptable or tolerable=>280 acceptable, tolerable, or not.	
			NOTE Risk evaluation assists in the decision about **risk treatment**.	
		281NEW	In some instances risk evaluation may simply be a decision rather than a process.	
			3.3.6.1 risk attitude	
			organization's approach to assess and eventually 287 retain, pursue, take or refuse **risk** (3.1)286=>turn away from risk	
			NOTE Risk appetite is used for positive response to a risk, risk aversion is used for negative response and risk attitude neutrally covers both cases.	
			3.3.6.2 risk appetite 291 limit =>293 tolerable risk	
			amount and 289DLtype of **risk** (3.1) an organization 291 stakeholder, or risk owners is prepared to pursue or take	
		292NEW	NOTE - Not applicable on safety aspects, human health, security and environmental protection aspects.	
			3.3.6.3 risk tolerance	
			organization's 297 stakeholdes, or risk owners readiness297=>ability to bear the **risk** (3.1) 296 without or after **risk treatment~~s~~** (3.3.7) in order to achieve its objectives	
			NOTE Risk tolerance can be limited=>298 affected by 299 overall external/internal context and applicable ~~legal or regulatory~~ requirements.	
			3.3.6.4 risk aversion	
			Attitude=>302 propensity to turn away from **risk** (3.1) 300 to a certain extent	

			3.3.6.5 risk aggregation	
			process ~~to combine~~ combining individual **risks** (3.1) DL303to obtain a more complete understanding of 304 or more synthetic view on **risk** (3.1) 306 to determine their collective influences.	
		305RP	process to combine individual risks to maximize potential benefit and minimize the potential losses	
			3.3.7 risk treatment	
			process of developing, selecting and implementing **controls** (3.3.5.9)	
		309RP	process of selection and implementation of measures to reduce the level of risk	
		310RP	process to modify risk	
			NOTE 1 Risk treatment can involve:	
			— avoiding the **risk=>309 risk avoidance** by deciding not to start or continue with the activity that gives rise to the **risk**;	1
		316DL	— 309risk acceptance :314DLseeking an opportunity by deciding to start or continue with an activity likely to create or enhance the **risk** 309 or retaining the risk by choice;	2
			— removing the source of the **risk**=>318 risk source; 309(risk elimination) — =>319 removing the rook cause of risk	3
			— changing the nature and magnitude of **likelihood** 309 (risk reduction and prevention);	4
			— [changing the **consequences**] 309 risk mitigation: by reducing the extent of the consequences of a particular ris;	5
			— 309 risk sharing : sharing the **risk** with another party or parties; and	6
		311RP	— Establishing an agreement with one or more parties to share risk	
		317DL	— 309 risk retention: by retaining the **risk** by choice.	7
			NOTE 2 Risk treatments that deal with negative **consequences** are sometimes referred to as **risk mitigation**,	

			risk elimination, risk prevention, risk reduction, DL309 risk repression and risk correction.	
			3.3.7.1 risk acceptance	
			DL323informed 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~~ 325Accepted risks are subject to **monitoring** and **review**.	
		328NEW	NOTE 4 Risks are often accepted with a provision or reserve intended to increase the likelihood of success	
			3.3.7.2 risk avoidance	
			329 informed decision , 330 based on the **level of risk** (3.3.5.10), not to be involved in, or to withdraw from, an activity 332 in order not to be exposed to a particular risk based on the **level of risk** (3.3.5.10)	
		331RP	decision not to be involved in, withdraw from, or eliminate risk source.	
			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 treatment**~~s~~ (3.3.7) involving the agreed distribution of **risk** (3.1) with other parties=>336&337 stakeholders	
			NOTE 1 Legal or regulatory requirements can limit, prohibit or mandate **risk sharing**.	
			NOTE 2 Risk sharing can be carried out through DL338insurance or other forms of contract.	
			NOTE 3 Risk sharing can create new **risks** or modify existing **risks**.	
		340NEW	NOTE 4 Risk sharing is explicit, with a full understanding and agreement between parties and stakeholders. Transfer of risk is done with the explicit understanding and agreement of all parties and stakeholders.	
			3.3.7.4 risk financing	

			form of **risk treatments** (3.3.7) involving contingent arrangements for the provision of funds to meet=>344modify the financial **consequences** (3.3.5.3) ~~should~~ in case they occur	
			3.3.7.5 risk retention	
			346 consequence of acceptance 348 of possibilities of the benefit of gain, and/or those of 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**.	
		349-351	**3.3.7.6 risk mitigation**	
			measures taken to reduce an undesired **consequence** (3.3.5.3) 352&353 and/or its likelihood	
			3.3.7.7 residual risk	
			risk (3.1) remaining after **risk treatment**~~**s**~~ (3.3.7)	
			NOTE 1 Residual risk can contain unidentified **risk**.	
			NOTE 2 Residual risk is also known as retained **risk**.	
			3.3.8.1 360 risk management 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** 362 controls or treatment.	
			3.3.8.2 365 risk management review	
			activity undertaken to determine=>364 periodical determination of 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** 366	

			controls or treatment (See decision on comment 362).	
			3.3.8.3 risk reporting	
			form of communication intended to address=>367inform particular internal or external **stakeholders** (3.3.1.1) to provide=>367providing information regarding the current state of 386DL [**risk** (3.1) and its management 368 the risk management and/or specific related sub-processes.	
			3.3.8.3.1 risk register	
			record of=>371 and information about identified **risks** (3.1) 372 and risk management.	
		373	record of identified, known or potential risks	
		374	file of information regarding to a set of risks or idenfied risks	
			NOTE The term risk log is sometimes used instead of risk register.	
			3.3.8.3.2 risk profile =>380 risk cluster, risk category	
			description of a set of **risks** (3.1) 378 and their interactions 379 applying to a set perimeter of the organization	
			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 382 first party process for obtaining evidence and evaluating it objectively to determine the extent to which the **risk management framework** (3.2.1) 383 or any selected part of it is adequate and effective	
			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*	

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

- RISK (3.1)
  - RISK MANAGEMENT (3.2)
    - RISK MANAGEMENT FRAMEWORK (3.2.1)
    - RISK MANAGEMENT POLICY (3.2.2)
    - RISK MANAGEMENT PLAN (3.2.3)
      - RISK MANAGEMENT PROCESS (3.3)
        - COMMUNICATION AND CONSULTATION (3.3.1)
          - STAKEHOLDER (3.3.1.1)
          - RISK PERCEPTION (3.3.1.2)
        - ESTABLISHING THE CONTEXT
          - EXTERNAL CONTEXT (3.3.2.1)
          - INTERNAL CONTEXT (3.3.2.2)
          - RISK CRITERIA (3.3.2.3)
        - RISK ASSESSMENT (3.3.3)
          - RISK IDENTIFICATION (3.3.4)
            - RISK SOURCE (3.3.4.1)
            - EVENT (3.3.4.2)
            - HAZARD (3.3.4.3)
            - RISK OWNER (3.3.4.4)
          - RISK ANALYSIS (3.3.5)
            - UNCERTAINTY (3.3.5.1)
            - LIKELIHOOD (3.3.5.2)
              - EXPOSURE (3.3.5.2.1)
            - CONSEQUENCE (3.3.5.3)
            - PROBABILITY (3.3.5.4)
            - FREQUENCY (3.3.5.5)
            - RESILIENCE (3.3.5.6)
            - VULNERABILITY (3.3.5.7)
            - RISK MATRIX (3.3.5.8)
            - CONTROL (3.3.5.9)
            - LEVEL OF RISK (3.3.5.10)
          - RISK EVALUATION (3.3.6)
            - RISK ATTITUDE (3.3.6.1)

					RISK APPETITE (3.3.6.2)
					RISK TOLERANCE (3.3.6.3)
					RISK AVERSION (3.3.6.4)
					RISK AGGREGATION (3.3.6.5)
			RISK TREATMENT (3.3.7)		
				CONTROL (3.3.5.9)	
				RISK ACCEPTANCE (3.3.7.1)	
				RISK AVOIDANCE (3.3.7.2)	
				RISK SHARING (3.3.7.3)	
				RISK FINANCING (3.3.7.4)	
				RISK RETENTION (3.3.7.5)	
				RISK MITIGATION (3.3.7.6)	
				RESIDUAL RISK (3.3.7.7)	
			MONITORING AND REVIEW		
				MONITORING (3.3.8.1)	
				REVIEW (3.3.8.2)	
				RISK REPORTING (3.3.8.3)	
					RISK REGISTER (3.3.8.3.1)
					RISK PROFILE (3.3.8.3.2)
				RISK MANAGEMENT AUDIT (3.3.8.4)	

Proposals of terms to be included in Clause 3 of ISO 31000

Entry Number in CD2 of Guide 73					Term	Convenor's suggestion	IE	NEN	use in ISO 31000?	How many times?
3	1				risk	Include	IE	NEN1/2	YES	125
3	2				risk management	Include	IE		YES	85
3	2	1			risk management framework	Include	IE	NEN1/2	YES	10
3	2	2			risk management policy	Include	IE		YES	10
3	2	3			risk management plan	Include	IE		YES	3
3	3				risk management process	Include	IE	NEN1/2	YES	32
3	3	1			communication and consultation		IE		YES	9
3	3	1	1		stakeholder				YES	33
3	3	1	2		risk perception				NO	
3	3	2	1		external context			NEN2	YES	7
3	3	2	2		internal context			NEN2	YES	7
3	3	2	3		risk criteria	Include			YES	13
3	3	3			risk assessment		IE	NEN1/2	YES	5
3	3	4			risk identification		IE	NEN1/2	YES	3
3	3	4	1		risk source			NEN1	NO	
3	3	4	2		event			NEN1	YES	8
3	3	4	3		hazard				NO	
3	3	4	4		risk owner	Include			YES	1
3	3	5			risk analysis		IE	NEN1/2	YES	7
3	3	5	1		uncertainty	Include		NEN1/2	YES	5
3	3	5	2		likelihood	Include			YES	8
3	3	5	2	1	exposure				NO	
3	3	5	3		consequence			NEN2	YES	17
3	3	5	4		probability				NO	
3	3	5	5		frequency				NO	
3	3	5	6		resilience				NO	
3	3	5	7		vulnerability				NO	
3	3	5	8		risk matrix				NO	
3	3	5	9		control				YES	4
3	3	5	10		level of risk	Include			YES	7
3	3	6			risk evaluation		IE	NEN1	YES	7
3	3	6	1		risk attitude	Include			YES	1
3	3	6	2		risk appetite	Include			YES	2
3	3	6	3		risk tolerance				NO	
3	3	6	4		risk aversion	Include			YES	1
3	3	6	5		risk aggregation				NO	
3	3	7			risk treatment		IE	NEN1/2	YES	30
3	3	7	1		risk acceptance				NO	
3	3	7	2		risk avoidance				NO	
3	3	7	3		risk sharing				NO	
3	3	7	4		risk financing				NO	
3	3	7	5		risk retention				NO	
3	3	7	6		risk mitigation				NO	
3	3	7	7		residual risk				YES	4
3	3	8	1		monitoring				YES	13
3	3	8	2		review				YES	22
3	3	8	3		risk reporting				NO	
3	3	8	3	1	risk register				NO	
3	3	8	3	2	risk profile				YES	1
3	3	8	4		risk management audit				NO	

Comment No.	Proposed Entry Number				Terms	Definition
18					Organization	organizations are chartered bodies of employment or public service with capital assets at risk or intangible assets like professional standing or reputation at risk to harm or loss.
49					risk management performance assessment	
74					risk trigger	
74					risk estimation	
74					risk frution	
74					risk transfer	
74					risk communication	
74					contingency	
74					treat and opportunity	
121					consult	
147					establishing the context	establishing the context Processes that an organization conducts to build the interrelated conditions in which it exists regarding the management of risk (3.1). NOTE1 The interrelated conditions can include internal factors and external factors of an organization which can impacts on its actors of management risk. NOTE2 The context of an organization can't be build in one day, it need emend and perfect continually and iteratively.
148					risk contextualization	identification of the parameters within which the risk is to be managed, and of risk criteria
313	3	3	7	8	risk elimination	
313 386	3	3	7	9	risk prevention	measures taken to reduce the likelihood (3.3.5.2) that an undesired event (3.3.4.2) occurs
387	3	3	7	10	risk correction	to be defined in a more extensive way than the previous definition on CD Guide 73.
388	3	3	7	11	risk reduction	reduction of the frequency (3.3.5.5) of an unfavourable event (3.3.4.2) and/or its consequence (3.3.5.3) to zero
74 389					risk reduction	Measures to be taken to reduce the risk level, by reducing likelihood of consequences or both, of a particular risk
390	3	3	4	5	risk category	Refers to associate risks by source to a particular nature.
391	3	3	5	12	key risk indicator	Refers to risk metrics to evaluate exposure risk level

Comment No.	Proposed Entry Number				Terms	Definition
392					risk trend	extent to which the risk is increasing or decreasing over time along the two dimensions of "likelihood" and "consequence
393					opportunity risk	the failure to achieve value generating opportunities
394					inherent risk	Risk present before application of controls or treatments
395	3	3	7	X	inherent risk	risk without taking into account existing risk controls
396	3	3	7	X	risk cost	The amount of money necessary for treating possible consequences caused by a source of risk
397					risk culture	the overall result of individual and group values, attitudes, perceptions, competencies, and patterns of behavior that determine the commitment to, and the style and proficiency of, an organization’s risk management
398					organization	Any entity, grouping of people or individual person owning risk
399					risk management application levels	Risk management can be applied at many levels in an organisation, such as strategic level, and at operational and tactical levels. It may also be applied to specific projects to assist with decisions or to manage specific recognized risk areas
400					strategic risk management	Strategic risk management is used to identify a comprehensive set of internal and external factors that could compromise an organisation’s ability to achieve its overall objectives. For the private sector this translates into anything that could threaten commercial interests and profitability, and for the public sector it translates into anything that can threaten effective policy-making and implementation in the long term.
401					operational risk management	Operational risk management is the control of risk arising from an organisation’s business functions and from the practical implementation of the management strategy, and to determine the level of control necessary to deal effectively with the assessed risk in the medium term.
402					tactical risk management	Control and usage by individuals at their workplace in dealing with immediate situations and deciding which risks require greater controls in the short term
403					risk ranking	The allocation of a classification to the likelihood (3.3.5.2) and consequence (3.3.5.3) of a risk. This may be in the form of high, medium, low or a numeric classification on a scale of say, 1 to 5.

Comment No.	Proposed Entry Number				Terms	Definition
404					risk prioritarization	Prioritization of risks focuses on areas that are most likely to have the greatest impact to the organisation or entity, to identify the level of urgency for action.
405					qualitative risk analysis	A broad general analysis to determine whether a more extensive analysis such as Quantitative Risk Analysis is necessary. It provides means of comparing risks in terms of High, Medium and Low, and setting priorities.
406					quantitative risk analysis	The systematic development of numerical estimates of the expected probability (frequency) and/or severity (consequence) of potential adverse events associated with an operation based on scientific evaluation and mathematical techniques.
407					known risk	
408					unknown risk	
409					objective	An internal performance goal or expectation established by an organization.
410					areas of Impact	Financial, property, human health, or environmental conditions of the organization, risk owners, or stakeholders affected by risks.
411	3	3	5	11	overall level of risk to objectives	The level of risk to system objectives resulting from the effects of all risks within the system or impacting the system objectives from without
412					risk provision	A reserve appropriate to the objective under consideration that represents the impact on that objective of risk acceptance (3.3.7.1)
413					threat	A potential cause of an incident which may result in harm to a system or organization. [ISO/IEC 27002:2005][13335-1:2004]
414					asset	Anything that has value to the organization. [ISO/IEC 13335-1:2004] Something of value to the enterprise. [Octave:2003]
415					opportunity	a. A favorable or advantageous circumstance or combination of circumstances. b. A favorable or suitable occasion or time. (http://www.thefreedictionary.com/opportunity)