ISO/TC 176/SC 1
Concepts and terminology

Email of secretary: jadmussen@asq.org
Secretariat: ANSI (United States)

Ballot and Request for Comments on Risk Definition

Document type: Other committee ballot

Date of document: 2019-05-02

Expected action: VOTE

Action due date: 2019-06-03

Background:

Committee URL: https://isotc.iso.org/livelink/livelink/open/tc176sc1

ISO/TMBG/JTCG-TF 14
Revision of Annex SL

Email of convenor: nigelhcroft@sapo.pt
Convenorship: ABNT (Brazil)

Indicative ballot and request for comments on definition of risk

Document type: Other committee ballot

Date of document: 2019-04-25

Expected action: VOTE

Action due date: 2019-06-15

Background:

This indicative ballot and request for comments on the definition of risk is being sent out to all TF 14 members as follows:

- All TF 14 members from TC/SC/PCs with responsibility for a Type A Management System Standard
  - You are requested to ***consult with your committee*** and submit only ONE response to the ballot and ONE set of consolidated comments
- All TF 14 members from NSBs:
  - You are requested to submit only ONE response to the ballot and ONE set of consolidated comments ***after consultation with the relevant interested parties representing the viewpoint of MSS users in your country***

Before submitting your response, please ensure that you have:

1. read the guidance note to the ballot in this document
2. participated in or viewed a recording of the webinar provided by TC 262 to TF 14 members on the intent and content of ISO 31000 (or at least studied the slides of that webinar)

Committee URL: https://isotc.iso.org/livelink/livelink/open/

Indicative ballot and request for comments on Annex SL Definition of "Risk"

This request is being sent out to all TF 14 members as follows:

- All TF 14 members from TC/SC/PCs with responsibility for a Type A Management System Standard
  - You are requested to ***consult with your committee*** and submit only ONE response to the ballot and ONE set of consolidated comments
- All TF 14 members from NSBs:
  - You are requested to submit only ONE response to the ballot and ONE set of consolidated comments ***after consultation with the relevant interested parties representing the viewpoint of MSS users in your country***

Questions and answers:

No.	Questions	Possible answers
1) Comments	After reading the attached Guidance notes, would you be in favour of: a. Annex SL adopting the ISO 31000:2018 definition of "risk" in its entirety **OR** b. Approaching ISO/TMB to seek their approval to allow the current Annex SL definition of risk to remain	a or b
2) Comments	If the final decision regarding the definition of risk in Q1 is NOT according to your preference, would you be in favour of: a. Accepting the decision, and adapting the text of Annex SL accordingly to try to address your concerns **OR** b. Removing any definition of "risk" from Annex SL	a or b

BEFORE SUBMITTING YOUR RESPONSE, PLEASE ENSURE THAT YOU HAVE:

A) READ THIS GUIDANCE NOTE
B) PARTICIPATED IN OR VIEWED A RECORDING OF THE WEBINAR PROVIDED BY TC 262 TO TF 14 MEMBERS ON THE INTENT AND CONTENT OF ISO 31000

Background:

The formal definition of "risk" was the subject of intense debate during the development of the first version of Annex SL, and continues with this revision. The main problem relates to two key words of

the ISO 31000 definition (both ISO 31000:2009 and ISO 31000:2018) - "Effect of uncertainty ***on objectives***". The reasons these two words were deleted in the current Annex SL definition of "risk" revolve primarily around concerns expressed by some MSS committees that:

a) Including the phrase "on objectives" implies that risk determination is limited only to formally-defined "XXX" objectives as defined in HLS Clause 6.2. Some users may interpret "objectives" widely, including the overall "intended outcomes of the management system" but others may interpret it more narrowly.
b) A consequence of (a) is that if an organization does not define objectives (in whatever form) for a specific activity or process, then it is difficult for auditors (and others) to require these to be subject to a determination of risk.
c) For some committees (specifically those dealing with topics that need to address regulatory issues, such as in Medical Devices), the main focus is on risks related to the process and product and less on "organizational" risks. These sectors typically apply the definition of risk in ISO Guide 51 (or similar ones set by government): "combination of the probability of occurrence of harm and the severity of that harm"

During the first meeting of TF 14 in Atlanta at the end of February 2019, three main topics related to "risk" were extensively debated.

- ***The definition of "risk" (the object of this request for comments***)
- Use of the phrase "risks and opportunities" that implies these are somehow "opposites", and confusion among users of the "positive effects of risk". The question of how to deal with "opportunities" (and the possible relationship with "threats" and/or "hazards") is ***NOT*** part of this request for comment, but will be subject to further discussion within TF14 before making specific proposals on whether or not to "decouple" the two words in the phrase "risks and opportunities". Any changes would be included in the first draft of the proposed revision and circulated for comment at that time.
- The deployment of "risk" beyond Clause 6.1 of Annex SL (into, for example, Clauses 8, 9 and 10, as well as "upwards" into clause 4). This topic is also ***NOT*** part of this request for comment, and will be discussed further by TF14 before the first draft of the proposed revision is circulated for comment.

About this request for comment:

Several possible scenarios were envisaged and discussed during the TF 14 meeting regarding the definition of "risk", but without reaching any consensus. We are now seeking wider input. Please read Attachment 1 to this Guidance note before proceeding.

The options we have available include:

1) **Adopt the ISO 31000:2018 definition in its entirety**
    a. We understand that this is the option preferred by ISO/TMB, in order to promote greater consistency among ISO standards (there are currently 40+ different definitions of "risk" in use)
    b. There are strong concerns among MSS committees about the use of this definition, for the reasons given above regarding the phrase "….. on objectives".
    c. Some changes to the text of the HLS and its guidance would probably be needed to maintain the intended meaning, and to minimize the potential for misinterpretation.

    NOTES:

- The ISO 31000 definition of "risk" has to be read in conjunction with the Annex SL definition of "objective" (see Attachment 1 to this document)
- TF14 / JTCG would have flexibility to add additional notes to the ISO 31000 definition of risk, and complete flexibility to revise the definition of "objective" (which is an "Annex SL definition") and the Guidance Notes to Appendix 2 (currently provided in Appendix 3 of Annex SL)

2) Approach TMB to seek their approval to allow the current Annex SL definition of risk to remain

a. This is the preferred option of a number of MSS committees, for the reasons given above regarding the phrase "….. on objectives". It was also the clear preferred option in an initial "straw poll" of the experts present during the February TF 14 meeting.
b. This option would, in principle, be the "default" ("no change to Annex SL"), but would require a justification to be submitted to ISO/TMB to explain the reasons for not adopting the ISO 31000:2018 definition.

NOTES:

- TF14 / JTCG would have full flexibility to revise the Guidance Notes to Appendix 2 (currently in Appendix 3 of Annex SL) in order to provide greater clarity (See Attachment 1 to this document)
- Some MSS have already deviated from Annex SL and opted to use the ISO 31000 definition of risk (examples include ISO/IEC 27001:2018, ISO 37001:2016, ISO 37101:2016, ISO 22301:2012, ISO 55001:2014, and ISO 18788:2015)

3) Remove any definition of "risk" from Annex SL

a. Do not include any definition of risk in Annex SL at all, while maintaining the concept of addressing risks in the text of Appendix 2.
b. This option would leave each MSS TC/SC/PC free to develop their own definition of risk, if required, with the "default" being that of ISO 31000:2018

4) Explore the possibilities to revise the ISO 31000 definition of risk

Some NSB-nominated experts in TF 14 who are involved in TC262 (Risk Management) commented that it might be possible to explore the potential willingness of TC 262 to modify their definition of risk to accommodate concerns of MSS TC/SC and PCs

NOTE from TF14 Convener: This option is not included in the request for comment because it is unlikely that it could be realized in a timely manner for the current revision of Annex SL

In the indicative ballot and request for comments, we are asking you two questions based on the above options (1 – 3), the responses to which will be used by TF 14 to define the next steps on this topic.

- **The first question asks respondents only to express their preference between the ISO 31000:2018 definition of risk and the current Annex SL definition.**

- **The second question aims to seek clarification on possible ways forward ONLY if the definition that is eventually agreed does not coincide with the respondents' preferred option.**

Whatever the result, you will have another opportunity to comment after the 1st draft of the Revision to Annex SL Appendix 2 and 3 is circulated (forecast for August 2019)

Attachment 1

Relevant definitions for consideration before providing your response

ISO 31000:2009 definition of "risk"

2.1
risk
effect of uncertainty 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** (2.17) and **consequences** (2.18), or a combination of these.

NOTE 4 Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated **likelihood** (2.19) of occurrence.

NOTE 5 Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood.

[ISO Guide 73:2009, definition 1.1]

Current Annex SL definition of "risk"

3.9
risk
effect of uncertainty

Note 1 to entry: An effect is a deviation from the expected — positive or negative.

Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

Note 3 to entry: Risk is often characterized by reference to potential "events" (as defined in ISO Guide 73:2009, 3.5.1.3) and "consequences" (as defined in ISO Guide 73:2009, 3.6.1.3), or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated "likelihood" (as defined in ISO Guide 73:2009, 3.6.1.1) of occurrence.

Note also that Appendix 3 of Annex SL provides additional guidance regarding the definition of "risk" as follows:

"Discipline specific standards can define "risk" in terms that are specific to their discipline. ISO 31000 provides a definition of "risk" that some discipline-specific standards can use (see also definition 3.09)."

ISO 31000:2018 definition of “risk”

3.1
risk
effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.

Note 2 to entry: Objectives can have different aspects and categories, and can be applied at different levels.

Note 3 to entry: Risk is usually expressed in terms of *risk sources* (3.4), potential *events* (3.5), their *consequences* (3.6) and their *likelihood* (3.7).

Annex SL definition of “objective”

(also important for this discussion, in case the decision is to adopt the ISO 31000:2018 definition of “risk”)

3.8
objective
result to be achieved

Note 1 to entry: An objective can be strategic, tactical, or operational.

Note 2 to entry: Objectives can relate to different disciplines (such as financial, health and safety, and environmental goals) and can apply at different levels [such as strategic, organization-wide, project, product and *process* (3.12)].

Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as an XXX objective, or by the use of other words with similar meaning (e.g. aim, goal, or target).

Note 4 to entry: In the context of XXX management systems, XXX objectives are set by the organization, consistent with the XXX policy, to achieve specific results.