INTERNATIONAL WORKSHOP AGREEMENT

IWA 31

First edition
2020-03

Risk management — Guidelines on using ISO 31000 in management systems

Reference number
IWA 31:2020(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

International Workshop Agreement IWA 31 was approved at a workshop hosted by BSI, held virtually by Zoom in December 2019.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

There is a steady growth in the number of organizations, of all types and sizes, that are using management systems based on an ISO and IEC Management System Standard (MSS)[1]. New ISO and IEC MSS continue to be developed to address specific aspects of an organization's activities, products or services. The ISO/IEC Directives, Part 1 specifies the high level structure (HLS) for MSS. This generic structure prescribes identical core text, common terms and core definitions for all ISO and IEC MSS. An organization can integrate requirements or recommendations of different MSS into their management system. The unified structure of MSS can make it easier for users to construct an integrated management system (IMS), rather than end up with a fragmented management system. All such MSS employ the concept of an approach based on risk management, a risk-based approach or risk-based thinking (depending on the terminology used within the management system in question), which is at the core of any management system. The main advantage of this is the holistic application of interrelated systems. ISO 31000:2018 can be used to further develop or improve an IMS through its guidance on how to determine the risks that need to be addressed to give assurance that the management system can achieve its intended outcomes, enhance desirable effects, prevent or reduce undesired effects, and achieve continual improvement.

ISO 31000 is international best practice regarding risk management, which is widely accepted, generic and open to manage any type of risk. Integrating risk management into its management system(s) by using ISO 31000 brings multiple benefits to an organization, whether they only address negative effects or include positive effects. The purpose of risk management as outlined in ISO 31000 is the creation and protection of value. It helps improve the decisions of risk owners or process owners and enhances the operations of processes and all other activities of the organization, including strategic and operational. This can lead to better results, higher output quality, less costly mistakes and the management of liability.

Integrating risk management in accordance with ISO 31000 creates and protects value in organizations by supporting the achievement of objectives and making the organization more resilient to adverse effects. Assessing risks enables their appropriate treatment and establishes a basis for increasing the effectiveness of the organization's management system, achieving improved results, and preventing negative outcomes. However, integrating risk management into a management system can pose challenges, which can be reduced by following the guidance in this document.

1) A list of ISO and IEC MSS is available at: https://www.iso.org/management-system-standards-list.html

Risk management — Guidelines on using ISO 31000 in management systems

1 Scope

This document gives guidelines for integrating and using ISO 31000 in organizations that have implemented one or more ISO and IEC Management System Standards (MSS), or that have decided to undertake a project implementing one or more MSS incorporating ISO 31000. This document explains how the clauses of ISO 31000 relate to the high level structure (HLS) for MSS.

This document does not provide guidance on implementing a management system in general. It does not specify requirements of a MSS. It does not provide a summary of ISO 31000; however, it does, as explained above, provide the background for understanding ISO 31000. Using this document does not remove the need to use other standards to address specific aspects of risk.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 31000:2018, *Risk management — Guidelines*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 31000:2018 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

4 The use of the term “risk” in ISO 31000 and other standards

The application of terminology should be taken in the context within which it is applied. For an organization’s risk management, ISO 31000:2018, 3.1, defines “risk” as the “effect of uncertainty on objectives”. Some standards do not refer to objectives, but the text regularly states that risks need to be addressed in order to give assurance that the management system can achieve its intended outcomes. An objective can be expressed as an intended outcome or result.

The risk management framework and process of ISO 31000 are customized and proportionate to the organization’s external and internal context related to its objectives. This includes the interested parties’ perspectives.

There are some contexts where different terminology is used (e.g. safety, occupational health and safety, medical devices sector). This use implements a general understanding of the term “risk” that narrows the ISO 31000 concept of risk in that it focuses on the potential negative impact of deviations from the expected. This approach can be considered to be included in the broader definition of risk in ISO 31000:2018, 3.1.

5 Guidance on ISO 31000 for users of MSS

ISO 31000:2018 offers guidance to all types of organizations, regardless of type and size, and is written for people who create and protect value in organizations by managing risks, making decisions, setting purpose and strategy, achieving objectives, and improving performance.

The eight principles of risk management act as a foundation for the creation and protection of value. These provide guidance on the characteristics of effective and efficient risk management, communicating its value, and explaining its intention and purpose. ISO 31000 provides a common approach to managing any type of risk faced by an organization throughout its life.

The purpose of the risk management framework is to assist the organization in integrating risk management into significant activities and functions. The effectiveness of risk management will depend on its integration into the governance of the organization, including decision-making.

The risk management process as set out in ISO 31000 should be customized proportionate to the external and internal context of the organization related to its objectives. It should be adapted so that it becomes an integral part of the management system, and is integrated into the structure, operations and processes of the organization.

Using the guidance on principles and framework, an organization may choose to customize the application of the risk management processes to its management system for any type of risk it faces throughout its life. Adding the steps of the risk management process can enhance the management system. In this context, it needs to be remembered that although the risk management process is often presented as sequential, in practice it is iterative.

Risk management should be applied whenever there is any information or estimation that initiates or adds to a process or activity, or whenever there is a change in the context of the organization.

There could be a degree of uncertainty in this information or estimation, which could have an effect on the achievement of objectives. An effect is explained in ISO 31000:2018, 3.1, as a deviation from the expected, which can be positive, negative or both. Therefore, the organization should revisit risk identification whenever there is new information or estimations relevant for its process and activities.

Figure 1 shows an overlay of the ISO 31000 guidelines with the framework of the generic HLS clauses for MSS. The top row references the HLS clauses and the left-hand column represents the ISO 31000 framework clauses. For example, looking at the intersection of ISO 31000:2018, 5.2, on leadership and the HLS clause on leadership, the grey key indicates there should be a process referring to the management of risk. Therefore, this table can be used as a reference point. For details on the clause connections, see Table A.1.

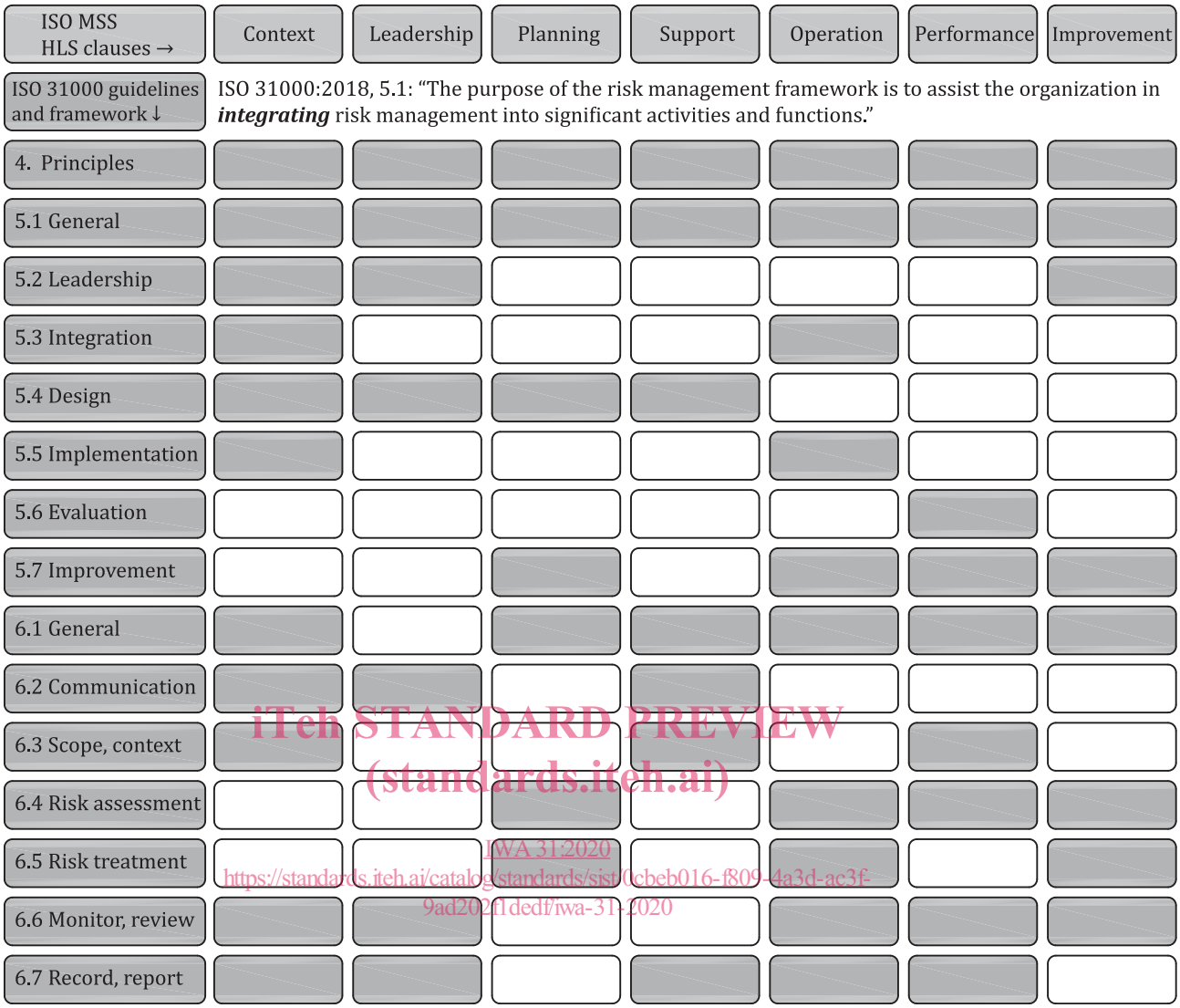

Figure 1 — Relationship between ISO 31000 and the clauses of the HLS for MSS

6 Integrated management systems and using ISO 31000

The application of risk management can be done through the process approach of a management system. The ISO 31000 framework should be merged with the management system by applying a gap analysis to include ISO 31000 framework components. By integrating risk management into the process approach, duplications or conflicts are avoided.

In order to achieve effective and efficient integration and implementation of the ISO 31000 framework and its process into other MSS, the organization should adopt ISO 31000 principles. The ISO Handbook *The Integrated Use of Management Systems Standards (IUMSS)*[5] could be a useful reference in this respect. For detailed steps for integrating the use of MSS, it is advised to refer to this handbook.

Annex A provides guidance on how on organization can approach the integration of management of risk into its MSS. Annex B is a case study of incorporating ISO 31000 into a multidiscipline management system.

Annex A
(informative)

Correspondence between ISO 31000 and the HLS for MSS

Table A.1 shows the linkages between the main clauses of ISO 31000 and the most important correlating clauses of the HLS for MSS. Users of ISO 31000 can integrate risk management practices into the management system of the organization where these clauses of the HLS are addressed.

Table A.1 — Correspondence between ISO 31000 and the HLS for MSS

Clauses of the HLS for MSS		Clauses of ISO 31000:2018		
		4. Principles[a]	5. Framework	6. Process
4. Context of the organization	4.1 Understanding the organization and its context	0, a), c), e), f), g)	5.2, 5.4.1	6.1, 6.3.1, 6.3.3, 6.3.4, 6.6, 6.7
	4.2 Understanding the needs and expectations of interested parties	0, a), c), d), e), f), g)	5.2, 5.4.1, 5.4.5	6.1, 6.2, 6.3.1, 6.3.3, 6.3.4, 6.6, 6.7
	4.3 Determining the scope of the XXX management system	0, a), c), f)	5.1, 5.2, 5.4.1, 5.5	6.3.1, 6.3.3, 6.3.4
	4.4 XXX management system	0, a), b), c), f)	5.1, 5.2, 5.3, 5.4.1, 5.5	6.3.1, 6.3.3, 6.3.4
5. Leadership	5.1 Leadership and commitment	0, a), c), d), g)	5.1, 5.2, 5.4.2, 5.4.4	6.2, 6.6, 6.7
	5.2 Policy	0, a), c), d), g)	5.2, 5.4.2	6.2, 6.6, 6.7
	5.3 Organizational roles, responsibilities and authorities	a), c), d), g)	5.2, 5.4.3	—
6. Planning	6.1 Actions to address risks and opportunities	0, a), b), e), f)	5.1, 5.4.2, 5.7.1	6.1, 6.4, 6.5
	6.2 XXX objectives and planning to achieve them	0, a), b)	5.4.2, 5.7.2	6.5
7. Support	7.1 Resources	0, a), f), g)	5.1, 5.4.4	6.3.4, 6.5.2
	7.2 Competence	0, a), f), g)	5.1	—
	7.3 Awareness	0, a), f), g)	5.1	—
	7.4 Communication	0, a), d), f)	5.1, 5.4.5	6.1, 6.2, 6.3.4
	7.5 Documented information	0, a), f)	5.1	6.1, 6.7
8. Operation	8.1 Operational planning and control	0, a), b), f)	5.1, 5.3, 5.5, 5.7	6.1, 6.4, 6.5, 6.6, 6.7
9. Performance evaluation	9.1 Monitoring, measurement, analysis and evaluation	a)	5.6	6.1, 6.3.3, 6.3.4, 6.4.1, 6.6, 6.7
	9.2 Internal audit	a)	5.6	6.1, 6.3, 6.4.1, 6.6, 6.7
	9.3 Management review	0, a), b), e), g)	5.6, 5.7	6.1, 6.3, 6.4.1, 6.6, 6.7
10. Improvement	10.1 Nonconformity and corrective action	0, a), h)	5.7	6.1, 6,4, 6.5, 6.6
	10.2 Continual improvement	0, a), h)	5.1, 5.2, 5.7	6.1, 6.4, 6.5, 6.6

[a] Principle “0” refers to the core principle “value creation and protection”.

NOTE The subclause numbers in the cells refer to the subclauses of ISO 31000:2018 according to relevant column heading.

Annex B
(informative)

Case study incorporating ISO 31000 into a multidiscipline management system

B.1 General

This case study illustrates a holistic approach for risk management in an organization, across multiple disciplines, based on the principles of ISO 31000 and the HLS for MSS. This case study does not provide any guidance on how to approach the integration of ISO 31000 into an organization's management system(s). It also does not include requirements related to each of the referenced MSS.

For the purpose of this annex, only the aspects of some clauses/requirements (those considered particularly effective) are highlighted to show how the application of requirements to the quality management system (QMS) processes of the organization were reviewed in the light of a risk management approach.

The text used in the case study represents the following:

— *italic text*: provides the perspective of the organization;

— regular text: provides guidance.

NOTE In this annex the term "interested party" has been used because it is the term used by this organization, which has applied ISO 9001 since 1997. According to the definition of "stakeholder" in ISO 31000:2018, 3.3, the term "interested party" can be used as an alternative.

B.2 Description and background of the organization

"XYZ" is a fictional organization used for the purpose of this annex.

— It comprises about 120 people.

— It concerns the development, trading, technical assistance and production, by mixing powders and liquids, of:

  — chemical products for material surface treatment;

  — chemical products for waters treatment;

  — lubricants for mechanical processing;

  — chemical auxiliaries;

  — temporary protective films and adhesive systems for the aerospace industry.

— It is a for-profit corporation.

— It needs to consider the regulatory environment, e.g. for the EU, Canada and Colombia, in regard to topics such as disposal requirements, chemical waste requirements, transportation requirements, safety requirements, etc.

— It has a distributed geography with two plants (Canada-Toronto and Colombia-Bogota) and one head office based in Brussels.