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 2020



COPYRIGHT PROTECTED DOCUMENT

© ISO 2020

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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 ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 The use of the term "risk" in ISO 31000 and other standards ... **1**
5 Guidance on ISO 31000 for users of MSS ... **2**
6 Integrated management systems and using ISO 31000 ... **3**
Annex A (informative) **Correspondence between ISO 31000 and the HLS for MSS** ... **4**
Annex B (informative) **Case study incorporating ISO 31000 into a multidiscipline management system** ... **5**
Annex C (informative) **Workshop contributors** ... **12**
Bibliography ... **14**

© ISO 2020 – All rights reserved

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.

© ISO 2020 – All rights reserved

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

© ISO 2020 – All rights reserved

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.

© ISO 2020 – All rights reserved