

PD ISO/TR 31004:2013



BSI Standards Publication

Risk management — Guidance for the implementation of ISO 31000

bsi.

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of ISO/TR 31004:2013.

The UK committee recognizes that ISO/TR 31004 has been developed in response to the need for additional guidance on the implementation of ISO 31000:2009 – *Risk management – Principles and guidelines*. The UK committee further recognizes this document's status as a Technical Report (TR). A TR is defined by ISO as "data of a different kind from that which is normally published as an International Standard". A TR is "entirely informative in nature" and does not "contain matter implying that it is normative" (ISO/IEC Directives, Part 1, Consolidated ISO Supplement, 2013).

In order to take advantage of material that has been drafted in committee so far, the ISO committee wished to publish this guidance as a TR at this stage, so as to offer guidance to organizations on ISO 31000. The report contains material that will be useful for organizations implementing ISO 31000.

The UK participation in its preparation was entrusted to Technical Committee RM/1, Risk management.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2013.
Published by BSI Standards Limited 2013

ISBN 978 0 580 75296 4

ICS 03.100.01

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 November 2013.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

TECHNICAL REPORT

PD ISO/TR 31004:2013

ISO/TR 31004

First edition
2013-10-15

Risk management — Guidance for the implementation of ISO 31000

*Management du risque — Lignes directrices pour l'implémentation
de l'ISO 31000*



Reference number
ISO/TR 31004:2013(E)

© ISO 2013



COPYRIGHT PROTECTED DOCUMENT

© ISO 2013

All rights reserved. Unless otherwise specified, 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
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

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 on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is Technical Committee ISO/TC 262, *Risk management*.

Contents		Page
Introduction		v
1	Scope	1
2	Normative references	1
3	Implementing ISO 31000	1
3.1	General.....	1
3.2	How to implement ISO 31000.....	2
3.3	Integration of ISO 31000 into the organization's management processes.....	3
3.4	Continual improvement.....	6
Annex A (informative) Underlying concepts and principles		7
Annex B (informative) Application of ISO 31000 principles		10
Annex C (informative) How to express mandate and commitment		21
Annex D (informative) Monitoring and review		25
Annex E (informative) Integrating risk management within a management system		34
Bibliography		37

Introduction

0.1 General

Organizations use various methods to manage the effect of uncertainty on their objectives, i.e. to manage risk, by detecting and understanding risk, and modifying it where necessary.

This Technical Report is intended to assist organizations to enhance the effectiveness of their risk management efforts by aligning them with ISO 31000:2009. ISO 31000 provides a generic risk management approach that can be applied to all organizations to help achieve their objectives.

This Technical Report is intended to be used by those within organizations who make decisions that impact on achieving its objectives, including those responsible for governance and those who provide organizations with risk management advice and support services. This Technical Report is also intended to be used by anyone interested in risk and its management, including teachers, students, legislators and regulators.

This Technical Report is intended to be read in conjunction with ISO 31000 and is applicable to all types and sizes of organization. The core concepts and definitions that are central to understanding ISO 31000 are explained in [Annex A](#).

[Clause 3](#) provides a generic methodology to help organizations transition existing risk management arrangements to align with ISO 31000, in a planned and structured way. It also provides for dynamic adjustment as changes occur in the internal and external environment of the organization.

Additional annexes provide advice, examples and explanation regarding the implementation of selected aspects of ISO 31000, in order to assist readers according to their individual expertise and needs.

Examples provided in this Technical Report might or might not be directly applicable to particular situations or organizations, and are for illustrative purposes only.

0.2 Underlying concepts and principles

Certain words and concepts are fundamental to understanding both ISO 31000 and this Technical Report, and they are explained in ISO 31000:2009, Clause 2, and in [Annex A](#).

ISO 31000 lists eleven principles for effective risk management. The role of the principles is to inform and guide all aspects of the organization's approach to risk management. Principles describe the characteristics of effective risk management. Rather than simply implementing the principles, it is important that the organization reflects them in all aspects of management. They serve as indicators of risk management performance and reinforce the value to the organization of managing risk effectively. They also influence all elements of the transition process described in this Technical Report, and the technical issues that are the subject of its annexes. Further advice is given in [Annex B](#).

In this Technical Report, the expressions "top management" and "oversight body" are both used: "top management" refers to the person or group of people that directs and controls an organization at the highest level, whereas "oversight body" refers to the person or group of people that governs an organization, sets directions, and holds top management to account.

NOTE In many organizations, the oversight body could be called a board of directors, a board of trustees, a supervisory board, etc.

Risk management — Guidance for the implementation of ISO 31000

1 Scope

This Technical Report provides guidance for organizations on managing risk effectively by implementing ISO 31000:2009. It provides:

- a structured approach for organizations to transition their risk management arrangements in order to be consistent with ISO 31000, in a manner tailored to the characteristics of the organization;
- an explanation of the underlying concepts of ISO 31000;
- guidance on aspects of the principles and risk management framework that are described in ISO 31000.

This Technical Report can be used by any public, private or community enterprise, association, group or individual.

NOTE For convenience, all the different users of this Technical Report are referred to by the general term “organization”.

This Technical Report is not specific to any industry or sector, or to any particular type of risk, and can be applied to all activities and to all parts of organizations.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 31000:2009, *Risk management — Principles and guidelines*

3 Implementing ISO 31000

3.1 General

This clause provides guidance to organizations seeking to align their risk management approach and practices with ISO 31000 and to maintain those practices in alignment on an ongoing basis.

It provides a general methodology that is suitable for application, in a planned manner, by any organization irrespective of the nature of its current risk management arrangements. This methodology involves the following:

- comparing current practice with that described in ISO 31000;
- identifying what needs to change and preparing and implementing a plan for doing so;
- maintaining ongoing monitoring and review to ensure currency and continuous improvement.

This will enable the organization to obtain a current and comprehensive understanding of its risks, and to ensure that those risks are consistent with its attitude to risk and its risk criteria.

Regardless of the motive for implementing ISO 31000, doing so is expected to enable an organization to better manage its risks, in support of its objectives. All organizations manage risk to some extent. The strategy for implementing ISO 31000 should recognize how an organization is already managing risk.