



DRAFT INTERNATIONAL STANDARD ISO/DIS 31000

ISO/PC 992

Secretariat: TMB

Voting begins on:
2008-04-01

Voting terminates on:
2008-09-01

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION

Risk management — Principles and guidelines on implementation

Management du risque — Principes et lignes directrices de mise en application

ICS 03.100.01

In accordance with the provisions of Council Resolution 15/1993 this document is circulated in the English language only.

Conformément aux dispositions de la Résolution du Conseil 15/1993, ce document est distribué en version anglaise seulement.

To expedite distribution, this document is circulated as received from the committee secretariat. ISO Central Secretariat work of editing and text composition will be undertaken at publication stage.

Pour accélérer la distribution, le présent document est distribué tel qu'il est parvenu du secrétariat du comité. Le travail de rédaction et de composition de texte sera effectué au Secrétariat central de l'ISO au stade de publication.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

© International Organization for Standardization, 2008

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

Copyright notice

This ISO document is a Draft International Standard and is copyright-protected by ISO. Except as permitted under the applicable laws of the user's country, neither this ISO draft nor any extract from it may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, photocopying, recording or otherwise, without prior written permission being secured.

Requests for permission to reproduce should be addressed to 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

Reproduction may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

16 **Contents**

Page

17	Foreword	iv
18	Introduction.....	v
19	1 Scope	1
20	2 Normative references	1
21	3 Terms and definitions.....	1
22	4 Principles for managing risk	1
23	5 Framework for managing risk	3
24	5.1 General	3
25	5.2 Mandate and commitment.....	4
26	5.3 Design of framework for managing risk	4
27	5.3.1 Understanding the organization and its context	4
28	5.3.2 Risk management policy	5
29	5.3.3 Integration into organizational processes	5
30	5.3.4 Accountability	5
31	5.3.5 Resources.....	5
32	5.3.6 Establishing internal communication and reporting mechanisms	6
33	5.3.7 Establishing external communication and reporting mechanisms.....	6
34	5.4 Implementing risk management	6
35	5.4.1 Implementing the framework for managing risk.....	6
36	5.4.2 Implementing the risk management process.....	7
37	5.5 Monitoring and review of the framework.....	7
38	5.6 Continual improvement of the framework.....	7
39	6 Process for managing risk	7
40	6.1 General	7
41	6.2 Communication and consultation.....	8
42	6.3 Establishing the context.....	9
43	6.3.1 General	9
44	6.3.2 Establishing the external context	9
45	6.3.3 Establishing the internal context.....	9
46	6.3.4 Establishing the context of the risk management process	10
47	6.3.5 Developing risk criteria	10
48	6.4 Risk assessment	11
49	6.4.1 General	11
50	6.4.2 Risk identification	11
51	6.4.3 Risk analysis	11
52	6.4.4 Risk evaluation.....	12
53	6.5 Risk treatment	12
54	6.5.1 General	12
55	6.5.2 Selection of risk treatment options	13
56	6.5.3 Preparing and implementing risk treatment plans	13
57	6.6 Monitoring and review	13
58	6.7 Recording the risk management process	14
59	Annex A (Informative) Attributes of enhanced risk management.....	15
60	A.1 General	15
61	A.2 Attributes	15
62	Bibliography.....	17
63		

64 Foreword

65 ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies
66 (ISO member bodies). The work of preparing International Standards is normally carried out through ISO
67 technical committees. Each member body interested in a subject for which a technical committee has been
68 established has the right to be represented on that committee. International organizations, governmental and
69 non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the
70 International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

71 International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

72 The main task of technical committees is to prepare International Standards. Draft International Standards
73 adopted by the technical committees are circulated to the member bodies for voting. Publication as an
74 International Standard requires approval by at least 75 % of the member bodies casting a vote.

75 This standard may be revised after 5 years on the basis of practical experience. Committees writing standards
76 are invited to inform the ISO Central Secretariat of any difficulties encountered with the implementation of its
77 provisions.

78 Introduction

79 Organizations of all types and sizes face a range of risks that can affect the achievement of their objectives.

80 These objectives can relate to a range of the organization's activities, from strategic initiatives to its
81 operations, processes and projects, and be reflected in terms of strategic, operational, financial and
82 reputational outcomes and impacts.

83 All activities of an organization involve risks. Risk management aids decision making by taking account of
84 uncertainty and its effect on achieving objectives and assessing the need for any actions.

85 Risk management process involves applying logical and systematic methods for:

86 — communication and consultation throughout the process;

87 — establishing the context;

88 — identifying, analyzing, evaluating and treating risk associated with any activity, process, function, project,
89 product, service or asset;

90 — monitoring and reviewing risk; and

91 — recording and reporting the results appropriately.

92 This International Standard recognizes the variety of the nature, level and complexity of risks and provides
93 generic guidelines on principles and implementation of risk management. To apply these generic guidelines in
94 a specific situation, this International Standard sets out how an organization should understand the specific
95 context in which it implements risk management.

96 Risk management can be applied to the entire organization, across its many areas and levels, at any time as
97 well as to specific functions and activities.

98 When implemented and maintained in accordance with this International Standard, risk management enables
99 an organization to, for example:

100 — encourage proactive rather than reactive management;

101 — be aware of the need to identify and treat risk throughout the organization;

102 — improve identification of opportunities and threats;

103 — comply with relevant legal and regulatory requirements and international norms;

104 — improve financial reporting;

105 — improve corporate governance;

106 — improve stakeholder confidence and trust;

107 — establish a reliable basis for decision making and planning;

108 — improve controls;

- 109 — effectively allocate and use resources for risk treatment;
- 110 — improve operational effectiveness and efficiency;
- 111 — enhance health and safety;
- 112 — improve incident management and prevention;
- 113 — minimize loss;
- 114 — Improve organizational learning; and
- 115 — Improve organizational resilience.
- 116 Risk management should ensure that organizations have an appropriate response to the risks affecting them.
117 Risk management should thus help avoid ineffective and inefficient responses to risk that can unnecessarily
118 prevent legitimate activities and/or distort resource allocation.
- 119 To be effective within an organization, risk management should be an integrated part of the organization's
120 overall governance, management, reporting processes, policies, philosophy and culture.
- 121 The same risk management approach can be adopted for all activities of an organization including projects,
122 defined functions, assets, and products or activities and will in turn strengthen the linkages between these
123 activities and the organization's overall objectives.
- 124 This International Standard is intended to be used by a wide range of stakeholders including:
- 125 — those responsible for implementing risk management within their organization;
- 126 — those who need to ensure that an organization manages risk;
- 127 — those who need to manage risk for the organization as a whole or within a specific area or activity;
- 128 — those needing to evaluate an organization's practices in managing risk; and
- 129 — developers of standards, guides, procedures, and codes of practice that in whole or in part set out how
130 risk is to be managed within the specific context of these documents.
- 131 Many organizations' existing management practices and processes include components of risk management
132 and many organizations have already adopted a formal risk management process for particular types of risk or
133 circumstances. Management can decide to critically review their existing practices and processes in light of
134 this standard.
- 135 Although the practice of risk management has been developed over time and within many sectors to meet
136 diverse needs, a generic approach consisting of a framework of essential components can help to ensure that
137 risk is managed effectively and coherently across an organization. The generic approach described in this
138 International Standard provides guidelines on implementing essential components for managing risk in a
139 transparent and credible manner within any scope and context.
- 140 Each specific sector or application of risk management brings with it individual needs, audiences, perceptions
141 and criteria. Therefore a key feature of this International Standard is the inclusion of "establishing the context"
142 as an activity at the start of this generic process of risk management. This feature will capture the diversity of
143 criteria as well as the nature and complexity of risk and other factors that need to be considered and managed
144 in each case.
- 145 Some areas of risk management within, for example, the areas of safety, human health and environment,
146 impose criteria that reflect an aversion to negative consequences. Such criteria can be contained in legal and
147 regulatory requirements and international norms. The application of the risk management approach described
148 in this International Standard helps to ensure that those criteria are identified and applied. Therefore, this

149 International Standard can also help an organization to comply with legal and regulatory requirements and
 150 international norms as well as to improve an organization's performance.

151 The relationship between the principles for managing risk, the risk management framework and the risk
 152 management process described in this standard is shown in Figure 1.

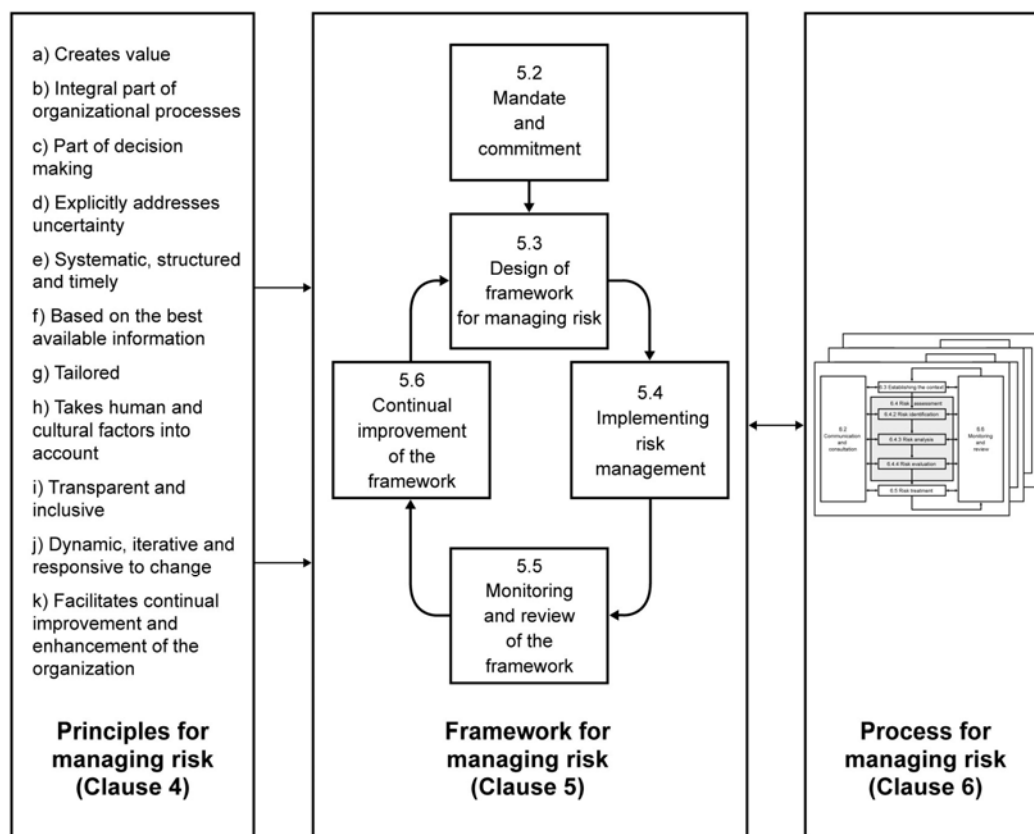


Figure 1 — Relationship between the risk management principles, framework and process

