STANDARDS Australia

AS/NZS ISO 31000:2009

Risk management—Principles and guidelines

STANDARDS NEW ZEALAND PAEREWA AOTEAROA

This Joint Australian/New Zealand Standard was prepared by Joint Technical Committee OB-007, Risk Management. It was approved on behalf of the Council of Standards Australia on 6 November 2009 and on behalf of the Council of Standards New Zealand on 16 October 2009.
This Standard was published on 20 November 2009.

The following are represented on Committee OB-007:

Australian Computer Society
Commerce Commission New Zealand
Committee IT-012
Department of Education and Early Childhood Development Victoria
Emergency Management Australia
Engineers Australia
Environmental Risk Management Authority New Zealand
Financial Services Institute of Australia
The Institute of Internal Auditors – Australia
Institution of Professional Engineers New Zealand
International Association of Emergency Managers
La Trobe University
Law Society of New South Wales
Massey University
Minerals Council of Australia
Ministry of Economic Development (New Zealand)
New Zealand Society for Risk Management
Risk Management Institution of Australasia
The University of New South Wales
University of Canterbury New Zealand

Keeping Standards up-to-date

Standards are living documents which reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued. Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments which may have been published since the Standard was purchased.

Detailed information about joint Australian/New Zealand Standards can be found by visiting the Standards Australia Web Site at www.standards.org.au or Standards New Zealand web site at www.standards.co.nz and looking up the relevant Standard in the on-line catalogue.

For more frequent listings or notification of revisions, amendments and withdrawals, Standards Australia and Standards New Zealand offer a number of update options. For information about these services, users should contact their respective national Standards organization.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Please address your comments to the Chief Executive of either Standards Australia or Standards New Zealand at the address shown on the back cover.

This Standard was issued in draft form for comment as DR 09063.

Australian/New Zealand Standard™

Risk management—Principles and guidelines

Originated as AS/NZS 4360:1995.
Third edition 2004.
Revised and redesignated as AS/NZS ISO 31000:2009.

Jointly published by Standards Australia, GPO Box 476, Sydney, NSW 2001 and Standards New Zealand, Private Bag 2439, Wellington 6140

ISBN 0 7337 9289 8

PREFACE

This Standard was prepared by Joint Standards Australia/Standards New Zealand Committee OB-007, Risk Management to supersede AS/NZS 4360:2004, *Risk management*.

When AS/NZS 4360:1999 was revised in 2004 (as part of a routine five yearly revision), it was decided by the Joint Australian/New Zealand Committee OB-007 that rather than undertake a similar revision in 2009, Standards Australia and Standards New Zealand would promote the development of an international standard on risk management which would then be adopted.

In 2005 the International Organization for Standardization (ISO) established a working group to develop the first international risk management standard using AS/NZS 4360:2004 as the first draft. The standard development process included extensive public consultation in Australia and New Zealand and resulted in the publication of ISO 31000:2009.

The main variations to AS/NZS 4360:2004, as outlined in the Introduction, are as follows:

(a) Risk is now defined in terms of the effect of uncertainty on objectives.

(b) The principles that organizations must follow to achieve effective risk management have now been made explicit.

(c) There is much greater emphasis and guidance on how risk management should be implemented and integrated into organizations through the creation and continuous improvement of a framework.

(d) An informative Annex describes the attributes of enhanced risk management and recognizes that while all organizations manage risk in some way and to some extent this may not always be optimal.

The process described for managing risk is identical to that in AS/NZS 4360:2004.

This Standard is identical with, and has been reproduced from ISO 31000:2009, *Risk management—Principles and guidelines*. Minor changes have been made to the Introduction to address the application of the Standard in Australia and New Zealand.

As this Standard is reproduced from an International Standard, the following applies:

(i) Its number does not appear on each page of text and its identity is shown only on the cover and title page.

(ii) In the source text ‘this International Standard’ should read ‘this Australian/New Zealand Standard’.

The term ‘informative’ is used to define the application of the annex to which it applies. An informative annex is only for information and guidance.

CONTENTS

Page

INTRODUCTION

Organizations of any kind face internal and external factors and influences that make it uncertain whether, when and the extent to which they will achieve or exceed their objectives. The effect this uncertainty has on the organization's objectives is "risk".

All activities of an organization involve risk. Organizations manage risk by anticipating, understanding and deciding whether to modify it. Throughout this process they communicate and consult with stakeholders and monitor and review the risk and the controls that are modifying the risk. This Standard describes this systematic and logical process in detail.

This is a new standard for managing risk that supersedes AS/NZS 4360:2004. It builds upon the processes contained in the superseded standard.

While all organizations manage risk to some degree, this Standard establishes a number of principles that need to be satisfied before risk management will be effective. This Standard recommends that organizations should have a framework that integrates the process for managing risk into the organization's overall governance, strategy and planning, management, reporting processes, policies, values and culture.

Risk management can be applied across an entire organization, to its many areas and levels, as well as to specific functions, projects and activities.

Although the practice of risk management has been developed over time and within many sectors to meet diverse needs, the adoption of consistent processes within a comprehensive framework helps ensure that risk is managed effectively, efficiently and coherently across an organization. The generic approach described in this Standard provides the principles and guidelines for managing any form of risk in a systematic, transparent and credible manner and within any scope and context.

The relationship between the principles for managing risk, the framework in which it occurs and the risk management process described in this Standard is shown in Figure 1.

When implemented and maintained in accordance with this Standard, the management of risk enables all organizations to, for example—

(a) increase the likelihood of achieving objectives;

(b) encourage proactive management;

(c) be aware of the need to identify and treat risk throughout the organization;

(d) improve the identification of opportunities and threats;

(e) achieve compatible risk management practices between organisations and nations;

(f) comply with relevant legal and regulatory requirements and international norms;

(g) improve financial reporting;

(h) improve governance;

(i) improve stakeholder confidence and trust;

(j) establish a reliable basis for decision making and planning;

(k) improve controls;

(l) effectively allocate and use resources for risk treatment;

(m) improve operational effectiveness and efficiency;

(n) enhance health and safety performance as well as environmental protection;

(o) improve loss prevention and incident management;

(p) minimize losses;

(q) improve organizational learning; and

(r) improve organizational resilience.

This Standard is intended to meet the needs of a wide range of stakeholders including—

(i) those accountable for achieving objectives and therefore ensuring that risk is effectively managed within the organization as a whole or within a specific area, project or activity;

(ii) those responsible for developing risk management policy within their organization;

(iii) those who need to evaluate an organization effectiveness in managing risk; and

(iv) developers of standards, guides, procedures, and codes of practice that in whole or in part set out how risk is to be managed within the specific context of these documents.

Organizations with existing risk management processes can use this Standard to critically review, align and improve their existing practices. Those whose risk management framework has been based on AS/NZS 4360:2004 will thereby benefit from the additional concepts and practices in this Standard.

In this Standard, the expressions “risk management” and “managing risk” are both used. In general terms, “risk management” refers to the architecture (principles, framework and process) for managing risks effectively, and “managing risk” refers to applying that architecture to particular risks.

AUSTRALIAN/NEW ZEALAND STANDARD

Risk management—Principles and guidelines

1 Scope

This International Standard provides principles and generic guidelines on risk management.

This International Standard can be used by any public, private or community enterprise, association, group or individual. Therefore, this International Standard is not specific to any industry or sector.

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

This International Standard can be applied throughout the life of an organization, and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets.

This International Standard can be applied to any type of risk, whatever its nature, whether having positive or negative consequences.

Although this International Standard provides generic guidelines, it is not intended to promote uniformity of risk management across organizations. The design and implementation of risk management plans and frameworks will need to take into account the varying needs of a specific organization, its particular objectives, context, structure, operations, processes, functions, projects, products, services, or assets and specific practices employed.

It is intended that this International Standard be utilized to harmonize risk management processes in existing and future standards. It provides a common approach in support of standards dealing with specific risks and/or sectors, and does not replace those standards.

This International Standard is not intended for the purpose of certification.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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.