HB 436:2004

RISK MANAGEMENT GUIDELINES

Companion to AS/NZS 4360:2004

STANDARDS AUSTRALIA

STANDARDS NEW ZEALAND
Paerewa Aotearoa

HB 436:2004
(Incorporating Amendment No. 1)

Handbook

Risk Management Guidelines Companion to AS/NZS 4360:2004

Originated as HB 142—1999 and HB 143:1999.
Jointly revised and redesignated as HB 436:2004.
Reissued incorporating Amendment No. 1 (December 2005).

Jointly published by Standards Australia International Ltd, GPO Box 5420, Sydney, NSW 2001 and Standards New Zealand, Private Bag 2439, Wellington 6020

ISBN 0 7337 5960 2

Preface

This Handbook provides generic guidance for establishing and implementing effective risk management processes in any organization. It demonstrates how to establish the proper context, and then how to identify, analyse, evaluate, treat, communicate and monitor risks.

This Standard incorporates Amendment No. 1 (December 2005). The changes required by the Amendment are indicated in the text by a marginal bar and amendment number against the clause, note, table, figure or part thereof affected.

This Handbook is based on the Joint Australian/New Zealand Standard, AS/NZS 4360:2004, *Risk management* (the Standard). Each Section contains an extract from the Standard, followed by practical advice and relevant examples.

This basic guide provides a generic framework for managing risk. It may be applied in a very wide range of organizations including:

- public sector entities at national, regional and local levels;
- commercial enterprises, including companies, joint ventures, firms and franchises;
- partnerships and sole practices;
- non-government organizations; and
- voluntary organizations such as charities, social groupings and sporting clubs.

It provides a reference for directors, elected officials, chief executive officers, senior executives, line managers and staff when developing processes, systems and techniques for managing risk that are appropriate to the context of their organization or their roles.

The contents are intended to provide only a broad overview of risk management. Organizations are expected to interpret this guide in the context of their own environments and to develop their own specific risk management approaches. Ultimately it is up to the risk makers and the risk takers to develop and manage their own risk management programmes.

Attributions

Standards Australia International acknowledges, with thanks, the contribution of the following organizations in the development of this Handbook:

Australian Computer Society

Australian Customs Service

Australia New Zealand Institute of Insurance and Finance

CSIRO (Commonwealth Scientific and Industrial Research Organisation)

Department of Defence (Australia)

Department of Finance and Administration

Emergency Management Australia

Environmental Risk Management Authority (New Zealand)

Institute of Chartered Accountants (Australia)

Institution of Engineers Australia

Institution of Professional Engineers New Zealand

Local Government New Zealand

Massey University (New Zealand)

Minerals Council of Australia

Ministry of Agriculture and Forestry (New Zealand)

Ministry of Economic Development (New Zealand)

NSW Treasury Managed Fund

New Zealand Society for Risk Management

Risk Management Institution of Australasia

Safety Institute of Australia

Securities Institute of Australia

University of New South Wales

Victorian WorkCover Authority

Water Services Association of Australia

Contents

Introduction

Risk management is a key business process within both the private and public sector around the world. Sound and effective implementation of risk management is part of best business practice at a corporate and strategic level as well as a means of improving operational activities.

This Handbook states in Clause 4.2 that risk is the chance of something happening that will have an impact on objectives. In English, usage of the word 'risk' usually has negative connotations, and risks are regarded as something to be minimized or avoided. In our more general definition, it is recognized that activities involving risk can have positive as well as negative outcomes. The processes described here can be used to identify and exploit opportunities for enhancing organizational outcomes as well as reducing negative consequences.

Risk management, as described here, is a holistic management process applicable in all kinds of organizations at all levels and to individuals. Readers should be aware that this usage of the term differs from a more restricted usage in some sectors. For example, in some areas the terms 'risk management' or 'risk control' are used to describe ways of dealing with identified risks, for which we use the term 'risk treatment'.

Some other terms used in this document also have different usages. For example the terms 'risk analysis', 'risk assessment' and 'risk evaluation' are variously used in risk management literature. They often have overlapping and sometimes interchangeable definitions, and they sometimes include the risk identification step. We have selected terminology that forms the basis of international standards.

Other handbooks have been developed that address applications of AS/NZS 4360 in specific areas (see Section 12).

In some areas there is a division of responsibility between those who carry out the analytical process of identifying and analysing risk and those who make the decisions about risk evaluation and the selection of actions to deal with identified risks. This is beneficial where it is important that risk analysis be seen to be independent, and possibly undertaken by technical specialists, with decision aspects of risk evaluation and selection of risk treatment options being the responsibility of senior decision makers. This guide does not deal with such divisions of responsibility, but they are compatible with the processes described here.

1 Scope and general

AS/NZS 4360:2004

1.1 Scope and application

This Standard provides a generic guide for managing risk. This Standard may be applied to a very wide range of activities, decisions or operations of any public, private or community enterprise, group or individual. While the Standard has very broad applicability, risk management processes are commonly applied by organizations or groups and so, for convenience, the term 'organization' has been used throughout this Standard.

This Standard specifies the elements of the risk management process, but it is not the purpose of this Standard to enforce uniformity of risk management systems. It is generic and independent of any specific industry or economic sector. The design and implementation of the risk management system will be influenced by the varying needs of an organization, its particular objectives, its products and services, and the processes and specific practices employed.

This Standard should be applied at all stages in the life of an activity, function, project, product or asset. The maximum benefit is usually obtained by applying the risk management process from the beginning. Often a number of discrete studies are carried out at different times, and from strategic and operational perspectives.

The process described here applies to the management of both potential gains and potential losses.

1.2 Objective

The objective of this Standard is to provide guidance to enable public, private or community enterprises, groups and individuals to achieve—

- a more confident and rigorous basis for decision-making and planning;
- better identification of opportunities and threats;
- gaining value from uncertainty and variability;
- pro-active rather than re-active management;
- more effective allocation and use of resources;
- improved incident management and reduction in loss and the cost of risk, including commercial insurance premiums;
- improved stakeholder confidence and trust;
- improved compliance with relevant legislation; and
- better corporate governance.

HB 436:2004 (Guidelines to AS/NZS 4360:2004) Risk Management Guidelines Companion to AS/NZS 4360:2004