STANDARDS Australia

AS/NZS 5050:2010

# Business continuity—
# Managing disruption-related risk

STANDARD

AS/NZS

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 14 May 2010 and on behalf of the Council of Standards New Zealand on 21 May 2010.
This Standard was published on 28 June 2010.

---

The following are represented on Committee OB-007:

Australian Computer Society
Australian Council of Trade Unions
Dairy Companies Association of New Zealand
Department of Education and Early Childhood Development Victoria
Emergency Management Australia
Engineers Australia
Environmental Risk Management Authority New Zealand
Financial Services Institute of Australasia
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
Safety Institute of Australia
Society for Risk Analysis, Australia and New Zealand Regional
The Institute of Internal Auditors, Australia
The University of New South Wales
University of Canterbury, New Zealand
Westpool

---

## 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 Standards may also be withdrawn.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 Web Shop at www.saiglobal.com.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 09013.*

Australian/New Zealand Standard™

# Business continuity—Managing disruption-related risk

First published as AS/NZS 5050:2010.



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

ISBN 978 0 7337 9615 9

# PREFACE

This Standard was prepared by Standards Australia/Standards New Zealand Committee OB-007, Risk Management to assist organizations maintain continuity of their business through effective management of disruption-related risk. This will thereby enhance an organization's resilience and can create strategic and tactical advantage in uncertain and volatile environments.

The approach to managing disruption-related risk described in this Standard (which incorporates concepts often described as 'Business Continuity Management' or 'BCM') is through application of AS/NZS ISO 31000:2009, *Risk management—Principles and guidelines*. Particular emphasis is given to disruptive events of such scale as to otherwise be beyond the capability of an organization's normal management system to cope with.

Managing this type of risk effectively requires a deep understanding of the organization's objectives, its operating environment and its dependencies.

The provisions of this Standard should be an integral part of the organization's plan for risk management. They will help reduce the occurrence and scale of events that could cause disruption as well as equipping the organization with the capacity to—

(a) stabilize any disruptive effects as soon as possible;

(b) continue and/or quickly resume those operations that are most critical to the organization's objectives;

(c) expedite a return to normal operations and a full recovery;

(d) capitalize on any opportunities created by the event; and

(e) assume additional risk with confidence.

The term 'informative' has been used in this Standard to define the application of the appendix to which it applies. An 'informative' appendix is only for information and guidance.

# CONTENTS

*Page*

# FOREWORD

All organizations must deal with change in the environments in which they operate. This may relate to changing stakeholder expectations, new strategies adopted by competitors, emerging technologies, changes in staff, availability of finance and the requirements of new legislation. Change is a constant and is best dealt with proactively rather than reactively.

To maintain business continuity, which is a core obligation of good governance, organizations must therefore anticipate and adapt to such changes to avoid either abrupt or progressive failure.

Ensuring business continuity requires a variety of conventional management techniques such as strategic and business planning, continual development of products and services, retaining and acquiring customers, recruiting new staff, raising finance, acquiring technologies and constant attention to quality and efficiency.

However, ensuring business continuity also requires effective management of the organization's risks, including the risks that arise from the possibility of disruptive events. Managing this particular risk to business continuity is the focus of this Standard.

**AS/NZS ISO 31000**

AS/NZS ISO 31000:2009, *Risk management—Principles and guidelines* is a globally accepted standard for managing all forms of risk.

It advocates that all risks should be managed in an integrated way, supported by an effective framework that sets policy, demonstrates commitment, provides resources, allocates responsibilities and constantly checks progress. It articulates principles for managing risk and also describes the same generic process for managing risks that, since AS/NZS 4360, *Risk management*, was first published in 1995, has been applied by organizations of all types in Australia and New Zealand.

The interrelationship of these elements of AS/NZS ISO 31000 (principles, framework and process) is illustrated in Figure 1.

**AS/NZS 5050:2010**

This Standard explains how to apply AS/NZS ISO 31000:2009 to disruption-related risks. It includes detailed guidance particular to the features of these risks and to the risk management framework through which they are managed.

The Standard therefore includes a methodology for determining how disruption can affect the continuity of the organization's business and the likelihood of those effects being experienced. This requires a deep understanding of the operating environment as well as a detailed grasp of the organization's objectives and risks. Particular attention is given to those activities, resources, processes and dependencies that are most critical.

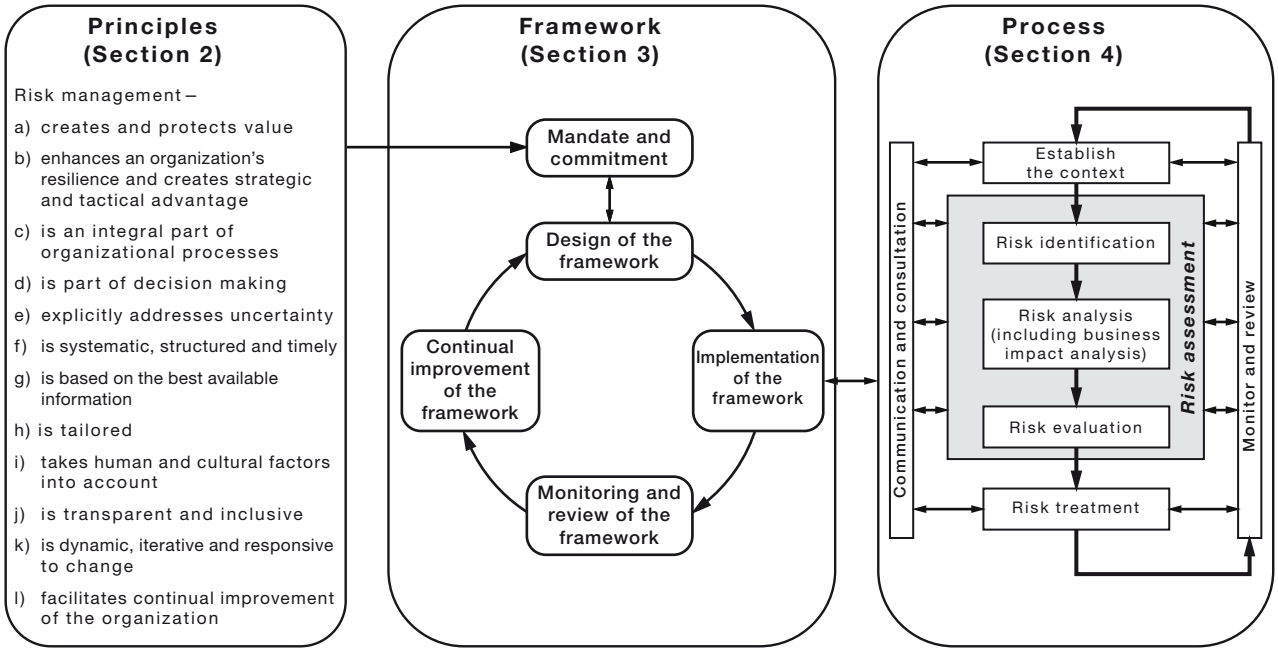


FIGURE 1 PRINCIPLES, FRAMEWORK AND PROCESS

The Standard recognizes that some potentially disruptive events may exceed, for some time anyway, the capacity of routine management methods and structures. It therefore explains how to prepare for this by building contingent capacity into the management framework and preparing contingency plans. This allows the organization to quickly change the mode of operations to help ensure business continuity despite occurrence of a potentially disruptive event. Such contingent capacity and plans enable management to quickly focus on stabilizing the situation and maintaining or resuming the most critical functions while still working in a planned way towards eventual restoration of routine operations and full achievement of objectives.

Unlike other guidelines and standards in Australia, New Zealand and elsewhere in the world that address disruption-related risk, AS/NZS 5050 does not limit its consideration of risk treatments to those that only apply once a potentially disruptive event has occurred. It also emphasises that ensuring business continuity in an efficient manner requires consideration of treatments that will reduce the occurrence and scale of events that could cause disruption. Such treatments should be part of the mix of risk treatments because the generally preferable path is not to be disrupted.

Even so, disruptions can sometimes create opportunities. The Standard advocates watching for and being in a position to exploit such possibilities. It also reminds organizations that the cumulative effect of small events, as well as large events can either cause or contribute to the severity of disruption—again emphasising the importance of deep and systematic thinking.

This Standard adopts the defined expressions of AS/NZS ISO 31000 and ISO Guide 73:2009 *Risk management—Vocabulary*. AS/NZS 5050 also uses expressions and language that have become familiar to those who work in this field where this is logical, and consistent with plain English. Together with a few additional definitions, this document standardizes the language used by those managing this type of risk and those managing other risks. This is particularly important if organizations are to succeed in the very important goal of an integrated approach to management of all types of risk.

The Standard includes a Section (5) for those organizations that wish to, or are required to, demonstrate formally that their framework and processes for managing disruption-related risk are able to meet the characteristics of management systems as described in ISO Guide 72[1]. Section 5 does not introduce any additional or different requirements for managing risk.

Figure 2 provides a sense of the relationships between the several areas of focus for managing disruption-related risk.

Before an event, there are opportunities to implement proactive controls that can make potentially disruptive events less frequent or severe, as well as making preparations for contingent controls that are activated once an event commences. These latter controls are aimed at reducing the scale and effects of disruption, returning to routine operations and a full recovery as soon as possible and seizing any opportunities that may arise.

The pre-event preparations include regular maintenance and exercising of the contingency plans and contingent capabilities that enable the organization to respond to the event in a practical and effective way, and transition back to routine management in a planned and controlled manner.

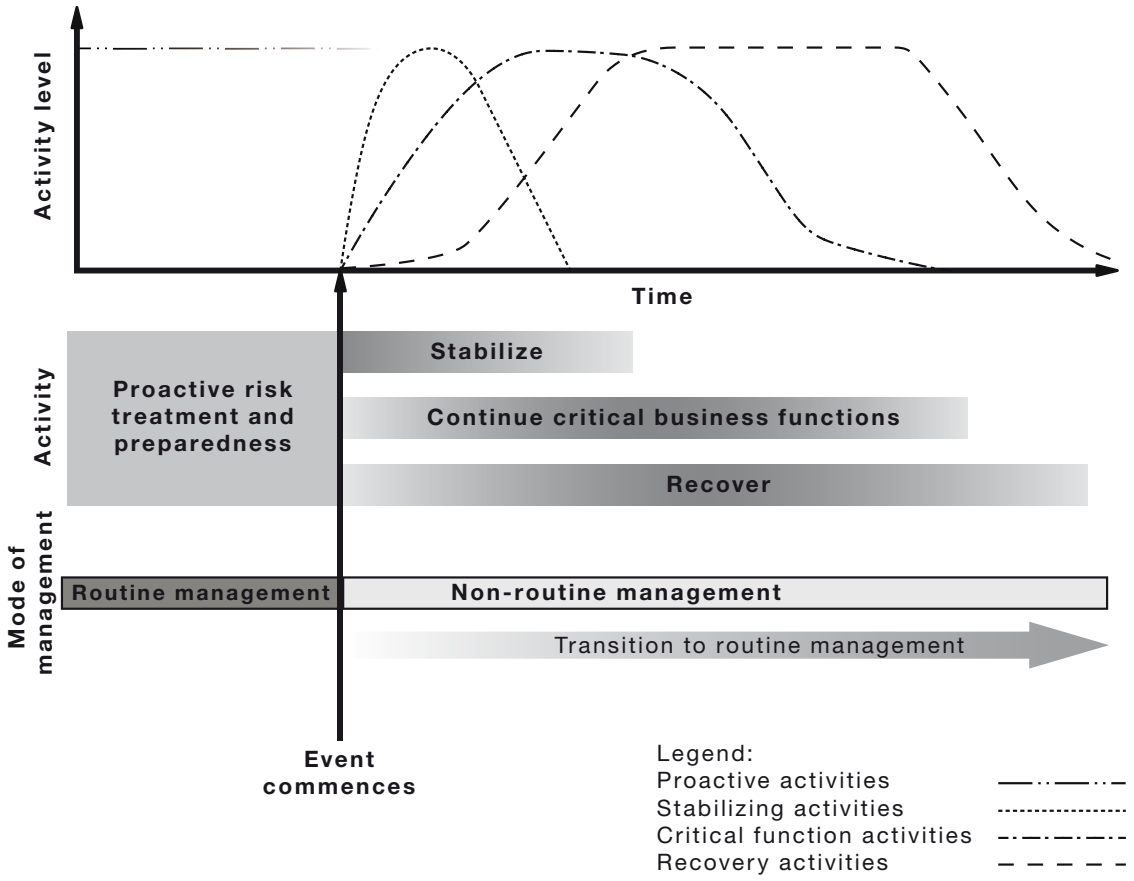


FIGURE 2 RELATIONSHIP OF TREATMENTS FOR DISRUPTION-RELATED RISK

[1] ISO Guide 72:2001, *Guidelines for the justification and development of management system standards.*

**Other Benefits Of Managing Disruption-Related Risk Effectively**

In contributing to maintaining business continuity, managing disruption-related risk also helps organizations to—

(a) demonstrate to internal and external stakeholders, their dependability and good governance;

(b) better understand their own business—sometimes thereby revealing opportunities to improve efficiency, governance and treatment of other risks;

(c) protect and advance brand value;

(d) protect the customer base and market share;

(e) have the confidence to accept further risk; and

(f) remain compliant with relevant legislative or other obligations.

The process of assessing and treating disruption-related risk can in itself contribute to or improve the adaptive capacity of the organization (i.e. its resilience). This occurs through—

(i) increasing awareness of the potential for disruption;

(ii) developing general skills as well as specific capacities which facilitate operating in a non-standard mode; while

(iii) maintaining a strong focus on objectives and critical activities.

STANDARDS AUSTRALIA/STANDARDS NEW ZEALAND

# Australian/New Zealand Standard
# Business continuity—Managing disruption-related risk

## S E C T I O N 1 S C O P E A N D G E N E R A L

### 1.1 SCOPE

The Standard describes the application of the principles, framework and process for risk management, as set out in AS/NZS ISO 31000:2009, to disruption-related risk. Managing such risk effectively will help maintain continuity of an organization's business[2]. The approach has drawn on, but of necessity goes beyond, many of the concepts that in the past may have been described as 'Business Continuity Management' or 'BCM'.

The Standard also includes, in Section 5, a schedule of requirements for those organizations seeking or required to demonstrate that their framework and processes for managing disruption-related risk are able to meet the characteristics of management systems as described in ISO Guide 72.

As is the case with AS/NZS ISO 31000, this Standard is applicable to all forms of organization[3].

### 1.2 REFERENCED DOCUMENTS

The following documents have been referenced in this Standard.

AS/NZS ISO
9000 Quality management systems—Fundamentals and vocabulary

31000 Risk Management—Principles and guidelines

ISO
Guide 72 Guidelines for the justification and development of management system standards

Guide 73 Risk management—Vocabulary

### 1.3 DEFINITIONS

For the purpose of this Standard, the following definitions apply.

#### 1.3.1 Activation

Process whereby all or a portion of a plan is put into effect.

#### 1.3.2 Assurance

Process involving monitoring and review that increases confidence and likelihood that planned objectives will be achieved.

#### 1.3.3 Audit

Process of systematic review against pre-determined criteria.

---

[2] 'Business' refers to the structure, processes and systems that organizations deploy to achieve their objectives.

[3] An 'organization' is any entity with objectives.