STANDARDS Australia

HB 158—2010

Delivering assurance based on ISO 31000:2009 Risk management – Principles and guidelines

handbook

HB

The IIA Research Foundation

The Institute of Internal Auditors Australia

Handbook

Delivering assurance based on ISO 31000:2009 Risk management—Principles and guidelines

Originated as HB 158—2002.
Revised and redesignated as GB 158—2004.
Revised and redesignated as HB 158—2006.
Second edition 2010.

Published by Standards Australia GPO Box 476, Sydney, NSW 2001, Australia

ISBN 978 0 7337 9489 6

PREFACE

This Handbook was prepared by a joint Working Group formed by the Institute of Internal Auditors – Australia (IIA - Australia) and the Joint Standards Australia/Standards New Zealand Technical Committee OB 007, *Risk Management*, and forms part of the series of publications based on ISO 31000:2009, *Risk Management—Principles and Guidelines*.

It was prepared to—

(a) help assurance providers to plan and implement their activities using the information arising from the (ISO 31000:2009) risk management process;

(b) advise assurance providers how to provide assurance over an organization's risk management framework and process when they are aligned to ISO 31000:2009;

(c) suggest a systematic approach to the design and assurance of controls;

(d) provide a common language and common processes for risk management specialists and auditors/assurance providers thereby enhancing communication between them and promoting risk management within their organizations.

Authors were—

(i) Pamela Finger, representing the Risk Management Institution of Australasia;

(ii) Andrew MacLeod of Brisbane City Council, representing the Institute of Internal Auditors – Australia;

(iii) Michael Parkinson of KPMG, representing the Institute of Internal Auditors—Australia; and

(iv) Grant Purdy of Broadleaf Capital International Pty Ltd, representing the Minerals Council of Australia.

This handbook builds on and is a companion to Standards Australia Handbook HB 254—2005, *Governance, risk management and control assurance*. That handbook draws linkages between objectives and risk management to suggest how a truly integrated risk management system that provides the foundation for sound governance can be created.

HB 254 provides a conceptual view of all forms of control assurance while this handbook gives a practical advice on how to plan and implement independent assurance.

The IIA Research Foundation recommends this handbook for its practical advice on how to plan and implement independent assurance and assess the adequacy of risk management framework and process in compliance with The IIA's International Standards 2010 *Planning*, 2100 *Nature of Work*, and 2120 *Risk Management*. It draws from The IIA's International Professional Practices Framework with respect to using and assuring the ISO 31000:2009 risk management process, and is a welcome addition to any research library.

In Australia ISO 31000:2009 is published as AS/NZS ISO 31000:2009.

CONTENTS

Page

Page

STANDARDS AUSTRALIA

HANDBOOK

Delivering assurance based on ISO 31000:2009 Risk management—Principles and guidelines

S E C T I O N 1 S C O P E A N D O B J E C T I V E S

1.1 GENERAL

This Handbook is a guide for internal auditors and any other assurance provider such as:

(a) External auditors.

(b) Information system control professionals – internal or external auditors and security professionals.

(c) Safety, health and environmental auditors.

(d) Quality auditors.

This Handbook draws on the revised HB 436[1], which is still to be published, and the IIA's[2] 'International Professional Practices Framework' (IPPF) with respect to using and assuring the ISO 31000:2009[3] risk management process. In particular, it describes how to use the risk management process to—

(i) develop a risk-based assurance strategy and program;

(ii) plan an assurance engagement;

(iii) report the assurance program; and

(iv) design controls.

The Handbook also provides a guide to assessing the adequacy of risk management framework and process. Following the processes in this Handbook will help organizations to assess whether management has designed and implemented the risk management and internal control system to manage the company's material risks and reported whether those risks are being managed effectively and provide analysis and independent appraisal of the adequacy and effectiveness of the company's risk management and internal control system[4]. It will also help internal auditors in particular comply with Standard 2010 (Planning), 2100 (Nature of Work) and 2120 (Risk Management) of the IPPF.

It is not the intention of this Handbook to provide guidance on the risk management process itself or to instruct internal auditors on their professional responsibilities.

---

1 Risk Management Guidelines: companion to ISO 31000:2009, Standards Australia, ISBN 0 7337 5960 2

2 Institute of Internal Auditors, Inc 247 Maitland Avenue, Altamonte Springs, Florida 32701-4201 U.S.A.

3 The international risk management standard ISO 31000:2009 *Risk Management—Principles and guidelines* may be published in local jurisdictions under a different designation. In Australia and New Zealand it is published as AS/NZS ISO 31000:2009.

4 ASX Corporate Governance Council- *Corporate governance principles and recommendations*, 2nd ed 2007 Principle 7: Recognise and manage risk.

1.2 ENTERPRISE RISK MANAGEMENT (ERM)

Enterprise-wide Risk Management or just Enterprise Risk Management is a term in common use. COSO[5] has defined it as: '*a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.*'[6]

Many organizations are moving to adopt consistent and holistic approaches to risk management and this document takes the approach that risk management is a management process that is, ideally, fully integrated into the management of the organization. It applies at all levels of the organization: enterprise level, function level or business unit level. Therefore this document does not generally distinguish ERM from any other form of risk management.

ISO 31000:2009 provides guidance for the framework of risk management within any organization. This framework is applicable for organizations of any size and may be used as a structural guide for practical application or evaluation of ERM.

1.3 TERMINOLOGY AND DEFINITIONS

1.3.1 Risk

The definition of risk from ISO 31000:2009 is used in this document.

Risk: *effect of uncertainty on objectives.*

Terms that are not otherwise defined in this document should be given their dictionary definition.

1.3.2 Assurance

In the context of internal auditing, Assurance Services are an '*objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, control processes for the organization*.'[7] Consistent with this we have, for the purposes of this document, defined:

Assurance: *a process that provides a level of confidence that objectives will be achieved within an acceptable level of risk.*

1.3.3 Inherent risk/Potential exposure

Financial reporting has long had a concept of **Inherent Risk** that has been defined as: '*the susceptibility of the subject matter information to a material misstatement, assuming that there are no related controls*'[8]

There seem to be several other general definitions for Inherent Risk commonly used. For example:

(a) '*The risk found in the environment and in human activities that is part of existence*.'[9]

(b) '*The likelihood that an accounting or auditing engagement will fail to comply with professional standards, assuming the firm does not have a quality control system*.'[10]

---

5 The Committee of Sponsoring Organizations of the Treadway Commission

6 'Enterprise Risk Management—Integrated Framework', COSO 2004

7 *International Professional Practices Framework* 2009, (IPPF) Glossary

8 AUS108.49 Framework for Assurance Engagements, Australian Accounting Standards Board, June 2004

9 David McNamee, MC2 Management Consulting, see www.pleier.com

10 http://www.nepr.org/risk.html