This is a free page sample. Access the full version online.

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

This is a free page sample. Access the full version online.

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.

COPYRIGHT

© Standards Australia Limited and the Institute of Internal Auditors—Australia

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher.

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

ISBN 978 0 7337 9489 6

This is a free page sample. Access the full version online.

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.

This is a free page sample. Access the full version online.

CONTENTS

Page

SECTION 1 SCOPE AND OBJECTIVES
1.1 GENERAL 5
1.2 ENTERPRISE RISK MANAGEMENT (ERM) 6
1.3 TERMINOLOGY AND DEFINITIONS 6

SECTION 2 SUMMARY OF THE RISK MANAGEMENT PROCESS
2.1 GENERAL 11
2.2 COMMUNICATE AND CONSULT 12
2.3 ESTABLISH THE CONTEXT 13
2.4 IDENTIFY RISKS 14
2.5 ANALYSE RISKS 15
2.6 EVALUATE RISKS 16
2.7 TREAT RISKS 17
2.8 MONITOR AND REVIEW 18

SECTION 3 RISK MANAGEMENT AND ASSURANCE
3.1 LINKING RISK MANAGEMENT TO ASSURANCE 20
3.2 STRATEGIC AND ORGANIZATION-WIDE APPROACHES TO RISK MANAGEMENT 21
3.3 ASSURANCE AND THE RISK MANAGEMENT PROCESS 22
3.4 ASSURANCE OF A RISK MANAGEMENT FRAMEWORK 23
3.5 INTERNAL AUDIT INVOLVEMENT IN RISK MANAGEMENT 26

SECTION 4 DEVELOPING AN ASSURANCE STRATEGY
4.1 GENERAL 28
4.2 STEP 1: IDENTIFYING THE ASSURANCE NEEDS OF THE ORGANIZATION 29
4.3 STEP 2: IDENTIFYING WHO THE ASSURANCE PROVIDERS ARE AND THEIR SCOPE OF OPERATION 29
4.4 STEP 3: IDENTIFY AND DOCUMENT ASSURANCE MECHANISMS 31
4.5 STEP 4: DESIGN THE ASSURANCE REVIEW PROGRAM 33
4.6 STEP 5: DEVELOP A RISK-BASED REVIEW PROGRAM 39
4.7 STEP 6: MEASURING THE STRATEGY 41

SECTION 5 PLANNING AN ENGAGEMENT
5.1 GENERAL 43
5.2 ENGAGEMENT SCOPE 43
5.3 ENGAGEMENT OBJECTIVES 43
5.4 ENGAGEMENT PROCEDURES 44
5.5 RATIONAL USE OF RESOURCES 44
5.6 SKILLS AND BODY OF KNOWLEDGE 45

SECTION 6 REPORTING ON THE ASSURANCE PROGRAM
6.1 GENERAL 46
6.2 REPORTING LINES 46
6.3 REPORTING THE INDIVIDUAL ASSURANCE ENGAGEMENT 47
6.4 ENSURING ACTION 49

This is a free page sample. Access the full version online.

Page

SECTION 7 DESIGNING AND IMPROVING CONTROLS
7.1 GENERAL 50
7.2 IDENTIFYING AND MEASURING CONTROL GAPS 50
7.3 DESIGNING CONTROLS 52
7.4 ADDING CONTROLS TO AN EXISTING PROCESS 55

SECTION 8 ASSURANCE OF THE RISK MANAGEMENT PROCESS AND FRAMEWORK
8.1 GENERAL 56
8.2 RISK MANAGEMENT PROCESS ELEMENT APPROACH 57
8.3 KEY PRINCIPLES APPROACH 59
8.4 MATURITY MODEL APPROACH 61

APPENDIX A EXAMPLE PRIORITY MODEL 64

SAI GLOBAL

This is a free preview. Purchase the entire publication at the link below:

Product Page

Looking for additional Standards? Visit Intertek Inform Infostore

Learn about LexConnect, All Jurisdictions, Standards referenced in Australian legislation