STANDARDS Australia

HB 254-2005

Governance, Risk Management and Control Assurance

This Australian Standard was prepared by Committee , Risk Management. It was approved on behalf of the Council of Standards Australia on 11 August 2005.
This Standard was published on 10 October 2005.

The following are represented on Committee :

Australian and New Zealand Institute of Insurance & Finance
Australian Computer Society
Business Continuity Institute
CSIRO Atmospheric Research
Department of Defence (Australia)
Department of Finance & Administration (Federal)
Emergency Management Australia
Engineers Australia
Environmental Risk Management Authority New Zealand
Institution of Professional Engineers New Zealand
Local Government New Zealand
Massey University
Minerals Council of Australia
Ministry of Agriculture and Forestry New Zealand
Ministry of Economic Development (New Zealand)
New Zealand Society for Risk Management
NSW Treasury Managed Fund
Property Council of Australia
Risk Management Institution of Australasia
Safety Institute of Australia (Incorporated)
Securities Institute of Australia
The University of New South Wales
Victorian WorkCover Authority

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 Standards may also be withdrawn.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 Standards can be found by visiting the Standards Web Shop at www.standards.com.au and looking up the relevant Standard in the on-line catalogue.

Alternatively, the printed Catalogue provides information current at 1 January each year, and the monthly magazine, *The Global Standard*, has a full listing of revisions and amendments published each month.

Australian Standards™ and other products and services developed by Standards Australia are published and distributed under contract by SAI Global, which operates the Standards Web Shop.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at mail@standards.org.au, or write to the Chief Executive, Standards Australia, GPO Box 476, Sydney, NSW 2001.

Handbook

Governance, risk management and control assurance

Originated as HB 254—2003.
Second edition 2004.
Third edition 2005.

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

ISBN 0 7337 6892 X

Preface

This Handbook was prepared by the Corporate Governance Working Group under the Joint Standards Australia/Standards New Zealand Technical Committee OB-007, Risk Management, and forms part of the series of publications based on AS/NZS 4360, *Risk management*. It supersedes HB 254—2004, *Guide to Controls Assurance and Risk Management*.

It was prepared to—

- provide guidance on the benefits to Boards from implementing an enterprise-wide risk management framework in their organisation; and
- outline the methodologies involved in implementing risk management and control assurance frameworks in support of sound governance.

Dr Ted Dahms, representing the Risk Management Institution of Australasia is the principal author of this Handbook.

Other key contributors, from Standards Australia's Joint Technical Committee on Risk Management, include—

- Dr Dale Cooper, representing the Securities Institute of Australia
- Mr Kevin Knight, representing the Risk Management Institution of Australasia
- Mr Grant Purdy, representing the Minerals Council of Australia.

Standards Australia would like to give particular acknowledgement to the contributions of the following organisations in the development of the Handbook—

- Australian National Audit Office
- Australian Stock Exchange
- Institute of Internal Auditors
- Queensland Audit Office

Contents

Page

Executive summary

Introduction

Traditional governance internal control and risk management guides are systems-based with a strong focus on legislative and regulatory compliance. Recent spectacular company failures however, indicate that compliance alone does not guarantee sound corporate governance. This Handbook outlines a Controls Assurance Plan for Boards and senior managers that refines and aligns current management practices to complement the more traditional compliance-based guides. It aims to promote amongst Directors, senior managers and employees—

- a sense of organisational and personal purpose; and
- capability and commitment in relation to the organisation's corporate objectives.

The philosophical foundation of the Controls Assurance Plan is the alignment of the risk management process with corporate governance by the—

- application of risk management process to objective setting at all levels of the organisation to develop controls that are at the same time strategies; and
- building of an underlying value system in the form of a self-sustaining system of inherent controls with a reduction in the reliance on formal compliance control.

The proposed system of inherent controls is developed by refining and aligning current management practices. This means that the Plan can be implemented within existing resources and without additional infrastructure. The leadership skill for the Board and senior managers is to achieve an effective balance between inherent and formal control appropriate for their organisation's level of control/risk maturity.

Although the Handbook is primarily designed with the private sector in mind, its concepts and frameworks are independent of legislative or regulatory constraints and can be applied with minimal modification in any jurisdiction, across all sectors including not-for-profits and to organisations of any size. Smaller organisations should keep their procedures simple and within the bounds of existing resources. The aim is to sharpen up, rather than add, resources to the risk management and control activities[1].

Where organisations do not have the resources to adequately fund an internal audit unit they need to implement alternative

---

[1] *Implementing Turnbull.* Institute of Chartered Accountants, England and Wales, 1999: p10.

procedures to provide control assurance to the Board. A methodology for providing Independent control assurance in smaller organisations is outlined in Clause 5.2 at the end of this Handbook.

Implementation of the Control Assurance Plan is facilitated by an appreciation of the relationship between governance frameworks and management practices together with an understanding of the linkages between governance, risk management and control.

Governance frameworks and management Practices

Essentially corporate governance is a guidance system composed of standard management practices operating within a governance framework designed to suit the organisation.

The Practices are essentially common management tools drawn together into a logical, interrelated system focused on achieving results. They can be universally applied to any organisation irrespective of their size, or statutory and regulatory environments.

Governance frameworks provide the structure within which the management practices operate. Parts of this structure are mandatory and set by legislation, regulation or listing rules in different jurisdictions, or by policy directives for public-sector organisations. Others are discretionary and set by Boards and senior management to address the management practices and can vary from organisation to organisation even within the same statutory environment. For this reason there is no one governance framework that suits all organisations, i.e. one size does not fit all.

Standard management practices are Control Activities for ensuring—

- corporate and operational objectives are developed and integrated throughout the organisation;
- competencies match objectives;
- clarity of roles and responsibilities;
- authority matches assigned responsibilities;
- high standards of ethical behaviour;
- effective monitoring and reporting systems; and
- effective and timely information flow throughout the organisation.

Goals and objectives–The focus

An understanding of the relationship between corporate governance, risk management, controls and strategies is fundamental to the successful implementation of the proposed Controls Assurance Plan. This relationship may be summarised as follows:

- Corporate governance is a guidance system for the achievement of planned objectives–it is an objectives-focused concept.
- Management of risk is part of each objective at all levels of the organisation.
- Risk management develops risk treatment plans that are at the same time the controls and strategies associated with achieving each objective.
- The meaning of control is broader than internal financial control and is expanded to include all planning and strategies put in place after the corporate objectives have been set. Transparency and probity are part of this control environment.
- The control environment provides reasonable assurance to Boards and senior managers that the organisational objectives will be achieved within an acceptable degree of residual risk.
- Corporate governance is an organisation's strategic response to risk[2].
- Reporting against performance measures for each objective is also a report on the effectiveness of strategies, controls and the risk management process for that objective. Risk management reporting is therefore part of performance reporting and not a separate exercise.

Effective risk management is therefore the cornerstone of sound governance and the Handbook provides an overview of the risk management process in line with AS/NZS 4360:2004, Risk management together with an implementation plan (Control Assurance Plan).

Benefits for the Board

The implementation of effective risk and control assurance frameworks provides a number of important outcomes in the corporate governance context, including:

- More effective strategic and operational planning with established linkages.
- Greater confidence in achieving planned operational and strategic objectives.
- Enhanced organisational resilience that reduces the time lost on 'fighting fires', and improves the organisation's potential to exploit opportunities.
- Greater confidence in the decision-making process.

---

[2] David McNamee and Georges Selim. *Changing the Paradigm* 2000. www.mc2consulting.com/riskart8.htm

- Improved stakeholder confidence leading to enhanced capital raising.
- Director protection.

Implementation

General

The principles underpinning an effective risk and control assurance framework are in essence standard management practices. Implementation, therefore, does not involve abandoning everything that is currently in place, but rather entails refining and aligning current practices.

The establishment of a risk and control assurance framework without an underlying value system encourages compliance rather than commitment. A compliance culture is neither responsive to change nor focused on innovation and performance improvement.

An underlying value system is set by inherent control, a central concept in the Control Assurance Plan, that has a different focus to formal control as follows:

- Inherent controls are proactive promoting purpose, capability and commitment throughout the organisation, including the Board, and are reliant on sound HR practices, ethics and communication. They occur continuously and consistently throughout the organisation as part of normal business practice and are to a large extent self sustaining. Elements that contribute to an inherent control system include systems thinking, developing a learning organisation, motivating trust and relationships, and matching competencies with objectives.
- Formal control involves assigning, monitoring, reviewing and reporting that are traditional command-control style processes based upon an organisational hierarchy.

The leadership skill for the Board, CEO and senior managers is to develop an effective balance between the two assurance processes. By increasing assurance through inherent controls, formal control can concentrate on areas of critical risk, the organisational focus becomes one of performance rather than compliance and the governance style is based upon an innovation–results model rather than command–control model.

An effective risk management framework

Framework

Risk management touches all of the organisation's activities. It is the foundation of the control environment and sound corporate governance. For this reason the implementation of an effective enterprise-wide risk management framework requires careful planning.

The risk management implementation plan proposed in the Handbook involves two phases as follows:

- An initial phase wherein the risk management implementation plan is developed and Board and senior management support is generated through processes such as policy development, information sessions and assigning risk management responsibilities to co-ordinators.
- An ongoing phase by which the risk management framework is—
    - embedded throughout the organisation as part of normal business practice; and
    - maintained through monitoring and reviewing risks, controls, and changes in the internal and external environments.

The Control Assurance Plan

The benefits to the Board from implementing an enterprise-wide risk management framework can be further improved by increasing the focus on inherent or in–built control and reducing the reliance on formal control. The Handbook outlines a Control Assurance Plan that provides a methodology for implementing Inherent control.

The focus of the Plan is five control elements (Figure 3) linked by an information system. These are:

- Planning (setting and communicating the purpose for the organisation).
- Board (shareholder representatives accountable for organisational performance to key stakeholders—sets organisational direction, develops broad policy and supervises management).
- Organisation (CEO, senior managers and employees—responsible for the delivery of organisation outputs in line with the Board's strategic objectives).
- Independent Assurance (provides risk management and control assurance to the Board independent of management—supports the Board's accountability).
- Management Assurance (management's risk and control assurance to the Board—supports management's accountability).

The Plan operates by addressing the control criteria of purpose, capability, commitment, monitoring and learning, and information in each Control Element according to the control assurance focus in each. The various aspects of the control criteria are addressed by applying standard management practices to each Control Element. The management practices are in essence Control Activities.

Control Activities address the Criteria in different ways in each Element depending upon the Element's control assurance focus. A high level methodology for aligning Control Activities with the

Criteria in each Element is set out in Section 4 in the form of a Control Assurance Plan.

Purpose

The Board is directly responsible for setting the organisation's strategic direction. It achieves this by developing the mission and vision from which are developed the corporate objectives. The Board is indirectly responsible through the CEO for ensuring that these objectives cascade throughout the organisation by translation into integrated and aligned operational, business, team and individual objectives. In association with this responsibility the Board and senior management have a duty to ensure that the significant internal and external risks associated with these objectives are identified and assessed.

Capability and Commitment

Capable and committed employees, teams and committees are the key to providing reasonable assurance that the organisation's objectives will be met within an acceptable degree of residual risk. Capability and Commitment are facilitated through communication and human resource strategies aligned to the corporate objectives. An important issue is the development of an awareness by all members of the organisation that they share the responsibility for the effectiveness of its risk management and control frameworks.

Monitoring and Learning

Effective monitoring and reporting processes maintain a watch over the achievement of objectives at all levels and ensure compliance within the organisation's statutory and policy environments. A key element in this area is ensuring the continuing effectiveness of the organisation's risk management and control frameworks. Learning is achieved through identification of non-compliance, post-event analysis, variances from planned targets and the identification of opportunities.

Information

Information plays a vital role in supporting the criteria of Purpose, Capability and Commitment that form the basis of inherent control. Similarly, information is the vital link in formal control through its support of effective decision-making, and monitoring and reporting against targets and critical risks.

The Handbook

The Handbook contains six Sections—

Section 1—examines the relationship of risk management, control and corporate governance.

Section 2—outlines the key benefits to the Board from ensuring that an appropriate system of risk management is in place.

Section 3—defines risk management, outlines the risk management process and provides an implementation plan for an enterprise-wide risk management framework.

Section 4—outlines a control assurance plan for Boards and senior managers, and introduces the concepts of inherent and formal control.

Section 5—contains advice on the practical implementation of a Control Assurance Plan.

Section 6—provides brief advice on managing change in order to achieve successful Control Assurance Plans.

The key messages in the Handbook are that—

- risk management is an essential tool underpinning all of the Board's functions, as well as assisting the Board to discharge its obligations;
- enterprise-wide risk management develops the organisation's control environment and strategies that support sound corporate governance;
- increasing reliance on inherent control over formal control reduces compliance costs and allows an increased focus on performance; and
- risk and opportunity for gain are partners, thus broadening the risk management process to opportunity identification and assessment.