



**The Institute of
Internal Auditors
Australia**

The voice of the profession

ASX Corporate Governance Guidelines IIA-Australia

**Guidance on implementing
Principle 7: 'Recognise and
Manage Risk' of the 2007
Edition of the ASX Corporate
Governance Principles and
Recommendations**

Copyright © The Institute of Internal Auditors Australia (IIA-Australia) April 2008. The text, graphics and layout of *Guidance on implementing Principle 7: 'Recognise and Manage Risk' of the 2007 Edition of the ASX Corporate Governance Principles and Recommendations* are protected by Australian copyright law and the comparable law of other countries. No part of this book may be reproduced, stored or transmitted in any form or by any means without the prior written permission of IIA-Australia except as permitted by law.

Disclaimer The Institute of Internal Auditors Australia and any persons involved in the preparation of this book expressly disclaim any and all contractual, tortious or other forms of liability to any person in respect of this book and any consequences arising from its use by any person in reliance on the whole or any part of the contents of this book. While care has been taken in the preparation of *Guidance on implementing Principle 7: 'Recognise and Manage Risk' of the 2007 Edition of the ASX Corporate Governance Principles and Recommendations*, the information contained herein is not intended to be advice and no person should act specifically on the information without first obtaining competent professional advice.

Contents

Introduction	5
What ‘risk management’ means under Revised Principle 7	6
Revised Principle 7 – how is it different?	7
Roles and responsibilities of key officers under Revised Principle 7	8
Implementation challenges of Revised Principle 7	10
Additional References	12
Implementation Checklist	14

Introduction

In August 2007, the ASX Corporate Governance Council (the Council) released its updated Corporate Governance Principles and Recommendations for listed companies.

The Principles and Recommendations recognise that there is no “one size fits all” approach to good governance and instead provides for an “if-not, why-not” regime. Under this regime, companies are able to undertake an alternative approach to that recommended provided they disclose how their approach addresses the spirit of each of the recommendations.

In updating the Principles and Recommendations, the Council was concerned that excessive guidance could be misconstrued as mandatory or quasi-law. To address this concern, a deliberate decision was made to keep guidance brief. This is consistent with the 2003 version of the Principles and Recommendations and IIA-Australia supports this approach.

Notwithstanding this decision, it is clear from the Council’s public consultation process and feedback from IIA-Australia’s membership that companies need practical guidance on what is appropriate in the areas of internal audit, internal control, risk management and management assurances.

As a key participant on the working groups dealing with these subjects and as the international thought leader in internal audit and internal control, IIA-Australia has developed this guidance to assist Directors, Chief Executives and Chief Audit Executives of Australian listed companies to address key issues arising from revised Principle 7.

In particular, this document highlights what is required to address the principal challenges presented by revised Principle 7, outlines the roles and responsibilities of key officers in setting the best approach for their organisation and canvasses other practical implementation matters.

What 'risk management' means under Revised Principle 7

Internal auditors, risk management professionals and internal control specialists bring a comprehensive and detailed approach to the task of risk management. This typically focuses on applying detailed, sometimes complex, risk management models to identify, evaluate and treat risk within an organisation. This level of rigour in many cases, uncovers hundreds of diverse risks across the organisation.

While this approach can manage risk comprehensively, it is quite different from the Council's requirement for risk management, as expressed in revised Principle 7. Organisations must therefore be mindful of these differences when focusing on Principle 7.



The two main points of difference in the Council's view of risk management are as follows:

1) Flexibility

The Council has not prescribed a particular risk management model or standard for organisations to follow in order to comply with revised Principle 7. Rather, organisations have the flexibility to design a risk management framework and structure that is most appropriate for their circumstances and this can be as simple or complex as the situation demands.

2) Materiality

The Council's focus is solely on the management of 'material business risks'. 'Material business risks' are described in the Council's *Supplementary Guidance to Principle 7* as "the most significant areas of uncertainty or exposure, at a whole-of-company level, that could have an impact on the achievement of company objectives". For the purposes of complying with revised Principle 7, organisations must therefore prioritise their risks with the aim of identifying a 'short-list' of the most significant risks. Organisations must appreciate this can be a more narrow and focused exercise than that ordinarily undertaken in a typical wide-ranging risk management project.

Revised Principle 7 – how is it different?

Prior to the 2007 update, the key requirements under Principle 7 were that:

- The board should establish and the organisation disclose, policies on risk oversight and management;
- The Chief Executive Officer (CEO) and Chief Financial Officer (CFO) should provide a written statement to the board that their certification regarding the integrity of the financial reports was founded on a sound system of risk management and internal compliance and control; and
- The CEO and CFO should provide a written statement to the board that the company's risk management and internal compliance and control system was operating efficiently and effectively in all material respects.

These requirements tended to confuse the oversight role of directors with the activities of management. It also placed a lot of emphasis on a risk management policy and on producing statements that risk management and internal control processes were in order. There was no accompanying requirement for management or other parties to verify whether those processes were operating well in reality so disclosures could have been statements of belief, unsupported by genuine investigation.

Revised Principle 7 clarifies the different roles of directors and management and shifts from a focus on disclosure to encouraging management to adopt more substantive risk

management activities. Some of the main changes include the following:

- Management must now report to the board on how effectively the organisation is managing its material business risks. This requires management to make judgements on what the material risks are and the level of effectiveness of risk management over them. This recognises that risk management is not absolute. There are no guarantees and the level of mitigation is a balance of perceived risk and reward;
- The board must now assess management's report on these 'material' matters in the same manner that it assesses other management reports on material matters. This will often include a request that management obtain independent assurance over the veracity of reporting on the organisation's systems for managing material business risks. In most cases, internal audit will be the party to assist management and the Board in obtaining an independent view, however external advisers may be engaged if appropriate.

Revised Principle 7 also steers organisations toward adopting practices that will help them form a robust and accurate view of how well they are handling their greatest business risks. This is a commendable change that will ultimately help organisations improve their performance and enhance the value of their business.

Roles and responsibilities of key officers under Revised Principle 7

Revised Principle 7 has defined and clarified the roles and responsibilities of key officers involved in the risk management process. These are outlined below in relation to each separate Recommendation:

Recommendation 7.1: 'Companies should establish policies for the oversight and management of material business risks and disclose a summary of those policies'.

Activity	Party Responsible
Identify all material business risks	Management
Establish policies for oversight and management of material business risks	Management
Determine the types and levels of risk that are acceptable to the organisation	Board
Review and assess policies on risk oversight, management and internal control	Board

Recommendation 7.2: 'The board should require management to design and implement the risk management and internal control system to manage the company's material business risks and report to it on whether those risks are being managed effectively. The board should disclose that management has reported to it as to the effectiveness of the company's management of its material business risks'.

Activity	Party Responsible
Design and implement the risk management and internal control system to manage the company's material business risks	Management (via the CEO)
Assess the level of effectiveness of the risk mitigation and internal control processes	Management
Report to the board on how effectively those risks are being managed	Management (via the CEO)
Assess management's report or judgement on the effectiveness of the implementation of the risk management and internal control system (at least annually)	Board
Disclose that management has reported on the effectiveness of the company's management of material business risks	Board
Provide independent appraisal of the adequacy and effectiveness of the company's risk management and internal control system on an annual basis	Internal Audit

Recommendation 7.3: ‘The board should disclose whether it has received assurance from the chief executive officer (or equivalent) and the chief financial officer (or equivalent) that the declaration provided in accordance with section 295A of the Corporations Act is founded on a sound system of risk management and internal control and that the system is operating effectively in all material respects in relation to financial reporting risks’.

Activity	Party Responsible
Disclose whether assurance has been received from CEO and CFO that the section 295A Corporations Act declaration is based on a sound system of risk management and internal control	Board
Assess the effectiveness of the risk management and internal control system in relation to financial reporting risks	CFO

Recommendation 7.4: ‘Companies should provide the information indicated in the Guide to reporting on Principle 7’.

Activity	Party Responsible
Disclose in the corporate governance statement in the annual report, explanations of any departures from Recommendations 7.1, 7.2, 7.3 or 7.4	Management and Board
Disclose in the corporate governance statement in the annual report, whether the board has received the report from management under Recommendation 7.2	Board
Disclose in the corporate governance statement in the annual report whether the board has received assurance from CEO and CFO under Recommendation 7.3	Board
Make publicly available, a summary of the company's policies on risk oversight and management of material business risks	Management

Implementation challenges of Revised Principle 7

Challenge No.1: How does management identify the 'material' risks and assess the effectiveness of risk management over them?

With management responsible for the design and implementation of an effective risk management system and for reporting accordingly to the Board, management needs to ask itself the following questions to test whether their obligations have been met:

- Are we satisfied that the material risks are identified?
- How are the material risks being assessed and measured?
- Is there regular monitoring and reporting to senior management and the board?
- Do the material risks all have mitigation plans? Are they effective in managing the material risks?
- Have we defined tolerance levels for the material risks?
- How do we measure and identify the indicators of risk?
- Are all material risks being escalated in a timely manner for decision making purposes? How do we know?
- How do we identify significant changes to the risks the organisation faces, including the identification of emerging risks?

Companies would benefit from having a common language around their material risks that is capable of comparing the spectrum of risks including currency, competition, finance control, compliance and other risks. It should be noted that risk management practices have generally not reached a high level of maturity where organisations have a well-understood common language across different risk areas.

This presents a challenge to implementing revised Principle 7 which, while requiring the identification of material risks, does not prescribe an integrated approach to compare and prioritise all risks across all areas. Devising a risk rating system to help identify and assess mitigation of risks is therefore one of the practical challenges for management in complying with revised Principle 7.

Challenge No.2: How does the Board assess the report from management?

Directors are required to exercise independent judgement in their oversight of how management is identifying and managing material risks and internal control systems. This review should be undertaken at least once a year.

Directors should therefore have satisfactory answers to the following questions in relation to the risk management report from management:

Implementation challenges of Revised Principle 7 Continued

- Is management's determination of material risks and related mitigation or exploitation strategies reasonable?
- Is management's assessment consistent with what we know about the organisation from other reports?
- Is management's assessment reasonable and appropriate for the industry?
- Is management's report sufficiently rigorous and supported by appropriate evidence?
- Are risk mitigation processes being actioned within the organisation?
- Are the mitigation processes working? How would we know if they were not?

Challenge No.3: How should independent appraisal of management's assessment of effectiveness be performed?

Revised Principle 7 highlights that directors may require assistance in evaluating management's assurances about the effectiveness of the risk management system.

Internal audit, with its close understanding of the organisation's overall operations, will generally be the most appropriate in-house resource to assist the board by providing an independent appraisal of the management report.

In making an independent assessment of the adequacy and effectiveness of the organisation's risk management and internal control systems, internal auditors would normally look at the following attributes:

- **Completeness** – Has management identified the material risks? Is the risk assessment approach consistent to identify the reasonably foreseeable material risks, or does it skew heavily towards risks which are already top of mind?
- **Prioritisation** – How robust is the process to prioritise risks across different areas of the organisation? Has the risk appetite and tolerance of the organisation been discussed, agreed and documented by management?
- **Reporting** – Are there appropriate protocols and controls, from the capture of relevant risk indicators and activities through to the reporting of the effectiveness of mitigation? Are the controls working and do the key elements of the report have integrity and reliability?
- **Mitigation** – Has management documented the mitigating strategies for the material risks in their area? Is accountability clear? Does management know whether the key controls are working?

Additional References

- **Monitoring** – Are risk assessments updated regularly? Are actions reviewed regularly for progress?
- **Culture** – Is there a culture of transparency, or is there a culture where bad news is not well received and therefore not reported?

Companies with robust risk management processes tend to provide more comprehensive disclosure of risks and associated mitigation strategies. Such companies often use disclosure as a means to build stakeholder confidence and reduce uncertainty as to their prospects and performance.

IIA-Australia supports greater transparency and disclosure around risk management in the interests of investors and wider stakeholders. Companies should view enhanced disclosure as a way to credibly establish their sustainability and performance credentials.



- **Institute of Internal Auditors Professional Practices Framework Standard 2100 and related Practice Advisory 2100-3** Internal Auditing's Role in the Risk Management Process.
- **AS/NZS 4360:2004 Risk Management**
- **“The Role of Internal Audit in Enterprise-wide Risk Management” IIA-UK ERM Position Statement** and adopted by The IIA Inc. September 2004.
- **Delivering Assurance based on AS/NZS 4360:2004 Risk Management Standard** published by Standards Australia (HB158-2006)



Implementation Checklist

In assessing the risk management framework, the internal auditor might consider the characteristics of a good risk management process as set out in HB158 A guide to the use of AS/NZS 4360, Risk Management, and the International Professional Practices Framework of the Institute of Internal Auditors:

It is systematic, structured and evidence based.

- There is a single organisation-wide risk management policy.
- The risk management process is recognised by management as its responsibility.
- Risk assessment mechanisms are uniform and well documented.
- All types of risk (both financial and non-financial) are considered and integrated into Board reporting.
- A hierarchy of risks is established so that the Board is informed about the most significant risks and management of risks occurs at an appropriate level in the organisation.
- Measurable and relevant risk indicators (including incident reports) are established.
- The risk management process has performance indicators that are routinely analysed and reported.

It explicitly addresses uncertainty and the causes of uncertainty.

- Risk assessment and risk management are integrated into planning processes.
- Risks arising from business strategies and activities are identified and prioritised.
- Procedures include root-cause analysis of identified risks.
- Mitigation strategies associated with approved plans are actively monitored and reported.
- Business cases include explicit consideration of uncertainty (risk) in calculation of costs and benefits.

It is an integral part of decision-making.

- Policy requires explicit risk assessments in association with significant business decisions.
- Such risk assessments address all options considered.
- Management and the Board set the risk appetite of the organisation.

Implementation Checklist Continued

It is dynamic, iterative and responsive to change.

- Risk monitoring mechanisms include a requirement to update risks and risk assessments should circumstances change.
- Incident reports and environmental scans are routinely used to identify new or emerging risks.
- The results of assurance activity (including internal audit) are used to confirm or adjust risk assessments.

It is transparent and understood by all interested parties through their inclusion and involvement in the process.

- All levels of the organisation receive training in the approved risk management process.
- The risk assessment involves relevant stakeholders at all levels of the organisation.
- Risk criteria reflect the perceptions and views of the relevant interested parties.

It is specific to the organisation and its external and internal context.

- Mechanisms are tailored to the organisation and its environment.
- Risk Management information is stored and managed centrally.
- The framework includes regular environmental scans to identify significant changes.
- The framework and mechanisms are routinely reviewed for continued relevance by Management and the Board.

It leads to the optimisation of control and maximisation of net benefit.

- Management assurance and internal audit activity includes consideration of the relevance and cost-benefit of controls.
- Costing models facilitate the measurement and comparison of risks.
- Assurance mechanisms test the correct operation of risk mitigation activity and controls.



**The Institute of
Internal Auditors
Australia**

The voice of the profession

For more information:

Telephone: +61 2 9267 9155 or 1800 236 366

Facsimile: +61 2 9264 9240

Email: enquiry@iia.org.au

Website: www.iia.org.au

IIA Australia:

**Level 7 / 133 Castlereagh Street
Sydney NSW 2000 Australia**