

ASX Corporate Governance Council

Revised Supplementary Guidance to Principle 7

30 June 2008

PRINCIPLE 7: 'Recognise and Manage Risk'

This Revised Supplementary Guidance should be read in conjunction with Principle 7 of the ASX Corporate Governance Council's (Council) *Corporate Governance Principles and Recommendations* (Principles and Recommendations) 2nd edition August 2007.

This Revised Supplementary Guidance is intended to assist companies seeking to develop appropriate risk management.

This Revised Supplementary Guidance does not impose any reporting obligations on companies.

Importance of risk oversight and control

A sound framework of risk oversight, risk management and internal control is fundamental to good corporate governance. It underpins reliable financial reporting, compliance with relevant laws and regulations, and effective and efficient operations.¹

The issue of risk is addressed in a number of the Principles, for example:

- the board's role in reviewing and ratifying risk management – Principle 1
- the management of issues relating to directors' independence and the maintenance of confidence in the company's financial integrity through codes of ethics and chief executive/chief financial officer assurance can be treated as governance risks - Principles 2, 3 and 4
- the risks associated with the legitimate interests of stakeholders; employees, creditors, the community, and others – Principle 3.

Since Council released the first edition of the Principles and Recommendations in 2003 an increasing number of companies have considered their frameworks of risk oversight and internal control and have disclosed details of these in their annual reports. There was a significant improvement in disclosure by companies of their risk management policies between 2004 and 2006.² Nonetheless, in 2006 over 30% of companies did not disclose information about their risk management policies. Council considers that this indicates further work is needed to encourage companies to report in a more meaningful way about risk.

Questions and answers

Principle 7 discusses the key components of risk oversight and management processes. Council considers that the following "Frequently asked questions" will assist companies and others to interpret the Principle.

¹ See COSO Definition of Internal Control at <http://www.coso.org/key.htm>

² See *Analysis of Corporate Governance Practices in 2004 Annual Reports*, ASX, May 2005 and also *2005 Analysis of Corporate Governance Practice disclosure*, ASX, May 2006 and *Analysis of Corporate Governance Practice Disclosure in 2006 Annual Reports*, all at www.asx.com.au/marketsupervision/corporategovernance.

What is a material business risk?

Material business risks are the most significant areas of uncertainty or exposure, at a whole-of-company level, that could have an adverse impact on the achievement of company objectives.³

Many business risks will be determined by the company's activities, the external environment and the nature of the company's assets. Factors that can influence a company's risk profile include:

- the industry sector outlook
- market share or size
- competition
- industrial relations
- foreign exchange and interest rates
- equity and commodity prices
- changes in government policy and regulation.

Companies will also have risks associated with their internal operating activities such as those arising from: OH&S, environmental impact, consumer protection/trade practices, financial controls and reporting, technology reliability, production capacity and people and skills.

What is a “system of risk oversight, risk management and internal control”?

Oversight of material business risks is a core function of the board. The board may choose to discharge this function with the assistance of one or more board committees. At a minimum, it includes:

- overseeing the establishment and implementation of an effective risk management and internal control system
- reviewing the effectiveness of that risk management and internal control system.

A system of risk oversight, risk management and internal control refers broadly to the collective policies, processes, structures and cultural values which companies establish to identify, assess, manage and monitor risks that may adversely affect the achievement of their business objectives.

A risk management system should not be created in isolation, but rather in conjunction with other business processes and systems, for example, the planning, budgeting and OH&S systems used to manage the company. The risk management system should include a description of:

- the company's risk management policies and procedures, including internal compliance and control, that can be made publicly available in accordance with Recommendation 7.1
- the board's risk oversight function
- the processes used to assess the effectiveness of the company's policies and procedures.

Companies may already have a risk management and internal control system or process which is consistent with the objectives of Principle 7. These companies are not asked to implement a new system, but to ensure that their system is designed to identify, assess, manage and monitor material business risks in a way that supports the achievement of their objectives.

³ This Guidance relates to Principle 7: however when companies consider the issue of material business risks, they need to be aware of their obligations under ASX Listing Rule 3.1 to make an announcement to the market in relation to some or all their material business risks and/or changes to those risks, where the risk or change is likely to have a material impact on the price or value of a company's securities. Boards will need to exercise their judgement when considering whether disclosure is required. Companies should also be aware of their obligations under Section 299A of the Corporations Act to include in the directors' report information required to make an informed assessment of companies' operations, financial position, business strategies and prospects for future financial years.

What are risk oversight and management and internal control policies?

Risk oversight and management and internal control policies should set out how the board and management discharge their responsibilities to exercise due care, diligence and skill in relation to the company's:

- reporting of financial information
- application of accounting policies
- financial management
- internal control systems
- business policies and practices
- protection of its assets
- compliance with relevant laws, regulations and standards.

Risk management and internal control policies should also set out how the board and management will assess whether:

- the company's internal processes for identifying, managing and reporting on material business risks are effective
- material business risks are reported regularly to the board
- the company's internal control and risk management system is reviewed as appropriate by management and by the internal and external auditors
- management has controls in place for unusual types of transactions that may carry risks
- senior executives, internal and external auditors and compliance staff understand the company's control environment.

What disclosures are required by Principle 7?

As indicated in the Guide to Reporting in Principle 7, companies are asked to disclose the following in the corporate governance statement in the annual report:

- explanation of any departures from Recommendations 7.1, 7.2, 7.3 or 7.4
- whether the board has received the report from management under Recommendation 7.2
- whether the board has received assurance from the chief executive officer (or equivalent) and the chief financial officer (or equivalent) under Recommendation 7.3

A summary of the company's policies on risk oversight and management of material business risks should be made publicly available, preferably in a clearly marked corporate governance section of the company website.

What disclosures are NOT required by Principle 7?

The following disclosures are NOT required by Principle 7:

- commercially sensitive information
- details of the company's material business risks.

Where a company discloses information elsewhere in the annual report or on its website it can cross-refer to that information to avoid duplicating disclosures.⁴

⁴ This Guidance relates to Principle 7: however when companies consider the issue of material business risks, they need to be aware of their obligations under ASX Listing Rule 3.1 to make an announcement to the market in relation to some or all their material business risks and/or changes to those risks, where the risk or change is likely to have a material impact on the price or value of a company's securities. Boards will need to exercise their judgement when considering whether disclosure is required.

What is the intended scope of the assurance from the chief executive officer/chief financial officer under Recommendation 7.3?

Council has clarified that the assurance provided by the chief executive officer/chief financial officer (or equivalent) to the board need only cover financial reporting risks and the associated controls, which underpin the integrity of the company's financial reporting. A statement about the provision of this assurance provides a level of information about the integrity of the processes that support financial reporting. This assurance is not intended to diminish senior executives' accountability in relation to other aspects of a company's risk management and control system.

What is meant by "operating effectively in all material respects" in the context of financial reporting?

The key test, which is indicative but not conclusive, of whether a risk management and internal control system is operating effectively in the context of financial reporting, is whether business outcomes are accurately reflected in financial reporting. The declaration required by Section 295A of the Corporations Act is that the company's financial records have been properly maintained, that the financial statements and the notes comply with the accounting standards and that the financial statements and the notes give a true and fair view.

Effective internal control processes will generally require some documentation of key financial reporting processes and evidence that key internal controls over material matters are operating satisfactorily. Typically, business outcomes are monitored through key performance indicators, financial and non-financial. However, events outside management's control can lead to unexpected outcomes. This would not necessarily mean that risk management is ineffective; management's ability to respond to unexpected outcomes will often reflect the effectiveness of a company's risk management policies and systems.

Assurance on the effectiveness of risk management and internal control is:

- intended to provide a reasonable but not absolute level of assurance to the board
- not intended to be a guarantee against adverse events, or losses, or more volatile outcomes.

Where a board receives an assurance from the chief executive officer and/or chief financial officer under Recommendation 7.3 which indicates that the company's risk management and internal control system is "operating effectively in all material respects in relation to financial reporting risks", but notes exceptions or areas of weakness which are not considered "material", there is no requirement for the Board to make a statement to this effect or to disclose the specifics of such qualifications under Recommendation 7.3.

However, if the board decides after reviewing the issues raised by the chief executive officer and/or chief financial officer in their assurance, that the internal control deficiencies are sufficiently material to raise serious questions about the integrity of the company's financial reporting, the board should consider whether action should be taken, such as considering continuous disclosure obligations under Listing Rule 3.1 or drawing these matters to the attention of the external auditor. The board should also consider carefully whether the financial statements and the directors' report can be signed without qualification.

What period of time should the sign-off cover?

Assurance in relation to financial controls should cover those controls in place during the entire reporting period to which the financial statements relate and up to the date of the assurance.

Where the assurance does not cover the entire period, perhaps due to a change of officer, the period of time covered and the reasons for this should be clearly disclosed.

Reporting

The purpose of reporting is to provide meaningful information to investors about the company's risk management policies and systems that could assist them in assessing the company.

To assist companies gain a practical sense of how to approach reporting in relation to Principle 7, Council has provided a hypothetical example of disclosure which it considers unhelpful and a hypothetical example which better addresses Principle 7. These examples are in Appendix A to this Supplementary Guidance. These examples are given solely to provide guidance on the appropriate level and depth of explanation – not for their content. Council would be concerned should any company simply copy these examples.

Sources of additional information

There is a range of guidance on risk oversight and management and internal control including:

- Australian / New Zealand Standard for Risk Management (AS/NZS 4360: 1999: Risk Management) at www.standards.com.au
- *Internal Control, Guidance for Directors on the Combined Code*, issued by The Institute of Chartered Accountants in England and Wales at www.icaew.co.uk
- *Recognise and Manage Risk: A Guide to Compliance with ASX Principle 7*, August 2008, Group of 100 Inc at www.group100.com.au⁵
- *Guidance on Implementing Principle 7: 'Recognise and Manage Risk' of the 2007 Edition of the ASX Corporate Governance Principles & Recommendations*, IIA-Australia, 2008 at www.iaa.org.au
- the United States-based Committee of Sponsoring Organisations of the Treadway Commission (COSO) publications about internal control and, more recently, enterprise risk management framework at www.coso.org
- the Institute of Internal Auditors and Standards Australia publication linking AS/NZS4360 on risk management to internal control at www.iaa.org.au.

⁵ Note that this replaces the previous Group of 100 publication *Guide to Compliance with ASX Corporate Governance Council Principle 7 – Recognise and Manage Risk* available on the Group of 100 website at www.group100.com.au.

APPENDIX A

Hypothetical example of unhelpful disclosure

Hypothetical unhelpful example A

The Audit and Risk Management Committee advises the Board on the establishment and maintenance of a framework of internal control, risk management and appropriate ethical standards for the management of the Group. The Audit and Risk Management Committee may also undertake other special duties as requested by the Board.

The responsibilities of the Audit and Risk Management Committee include:

- *reviewing the annual and half-year financial reports and other financial information distributed externally*
- *assessing company risk assessment processes*
- *assessing whether non-audit services provided by the external auditor are consistent with maintaining the external auditor's independence*

This disclosure is unhelpful. Although the company talks about an Audit and Risk Committee and comments that assessing company's risk management processes is part of the committee's responsibilities, there is no description of the company's risk management policies and systems or how accountability for these policies and the processes for oversight and management of material business risks is developed and overseen within the organisation. The example does not provide any indication of whether the company's approach to the management and oversight of material risks is effective or if not, whether the organisation is working towards this through the statements under Recommendations 7.2 and 7.3.

Hypothetical example of helpful reporting

The following is a hypothetical example of helpful disclosure. It should not be interpreted as indicating that Council endorses the practices set out in the example, any material referred to in it or considers that it contains any minimum standard that applies to all companies.

This is consistent with Council's view that companies need to have flexibility in relation to their corporate governance reporting. Council would be concerned should any company simply copy this example.

Hypothetical helpful example B

The identification and effective management of risk, including calculated risk-taking is viewed as an essential part of the company's approach to creating long-term shareholder value.

Management, through the Chief Executive, is responsible for designing, implementing and reporting on the adequacy of the company's risk management and internal control system. Management reports to the Audit and Risk Committee on the company's key risks and the extent to which it believes these risks are being managed. This is performed on a six monthly basis or more frequently as required by the Board or relevant subcommittee.

The Board is responsible for satisfying itself annually, or more frequently as required, that management has developed and implemented a sound system of risk management and internal control. Detailed work on this task is delegated to the board Audit and Risk Committee and reviewed by the full Board. The Audit and Risk Committee also oversees the adequacy and comprehensiveness of risk reporting from management.

As part of its duties, internal audit provides assurance to the Board Audit and Risk Committee and to management on the adequacy of the company's risk framework, and the completeness and accuracy of risk reporting by management.

A standardised approach to risk assessment is used across the Group to ensure that risks are consistently assessed and reported to an appropriate level of management, and to the Board if required.

The company carries out risk specific management activities in four core areas: strategic risk, operational risk, reporting risk and compliance risk in accordance with Australian / New Zealand Standard for Risk Management (AS/NZS 4360 Risk Management) and the Committee of Sponsoring Organisations of the Treadway Commission (COSO) risk framework.

Strategic and operational risks are reviewed at least annually by all operating divisions as part of the annual strategic planning, business planning, forecasting and budgeting process. Divisional risk profiles are also reviewed as part of the quarterly due diligence process within these divisions.

The company has developed a series of operational risks which the company believes to be inherent in the industry in which the company operates. These include:

- fluctuations in commodity prices*
- fluctuations in exchange rates*
- depletion of reserves*
- fluctuations in demand volumes*
- political instability/sovereignty risk in some operating sites*
- the occurrence of force majeure events by significant suppliers*
- increasing costs of operations, including labour costs*
- changed operating, market or regulatory environments as a result of climate change.*

These risk areas are provided here to assist investors to understand better the nature of the risks faced by our company and the industry in which we operate. They are not necessarily an exhaustive list.

Detailed internal control questionnaires are completed by all major divisions and key finance managers in relation to financial and other reporting on a six monthly basis. These are reviewed by our senior finance team and our external auditors as part of our half-yearly reporting to the market and to achieve compliance with section 295A of the Corporations Act

and Recommendation 7.3 of the ASX Corporate Governance Council's Corporate Governance Principles and Recommendations.

Through the General Counsel's office, a detailed compliance programme also operates to ensure the company meets its regulatory obligations. Executive management committees also meet regularly to deal with specific areas of risk such as OH&S, Treasury and environmental risk.

The Board also receives a written assurance from the Chief Executive Officer (CEO) and the Chief Financial Officer (CFO) that to the best of their knowledge and belief, the declaration provided by them 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 relation to financial reporting risks. The Board notes that due to its nature, internal control assurance from the CEO and CFO can only be reasonable rather than absolute. This is due to such factors as the need for judgement, the use of testing on a sample basis, the inherent limitations in internal control and because much of the evidence available is persuasive rather than conclusive and therefore is not and cannot be designed to detect all weaknesses in control procedures.

The company's internal audit function conducts a series of risk-based and routine reviews based on a plan agreed with management and the Audit and Risk Committee. In order to ensure the independence of the internal audit function, the head of internal audit meets privately with the Audit and Risk Committee without management present on a regular basis and is responsible for making the final decision on the head of internal audit's tenure and remuneration.

The company will provide updates on any changes in its circumstances in press releases on the investor section of the company's website.

This disclosure is considered helpful as it provides a comprehensive view on how the company approaches risk management and oversight. The disclosure also provides insights in relation to the risks in the industry in which the company operates.