

# ASX Corporate Governance Council Supplementary Guidance

2 August 2007

## PRINCIPLE 7: 'Recognise and Manage Risk'

This 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) 2<sup>nd</sup> edition August 2007.

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

**This 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.<sup>1</sup>

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 disclosure of incentive-related payments that encourage and reward risk taking - Principle 9
- the risks associated with the legitimate interests of stakeholders; employees, creditors, the community, and others – Principle 3.

Since Council released 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.<sup>2</sup> 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.

---

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

<sup>2</sup> 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/marketsupevision/corporategovernance](http://www.asx.com.au/marketsupevision/corporategovernance).

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

Risk oversight is a core function of the board, or the appropriate board committee, that complements a company’s approach to setting and executing strategy. At a minimum, it includes:

- overseeing the establishment and implementation of the risk management and internal control system
- reviewing the effectiveness of the company’s risk management and internal control system.

Risk oversight, risk management and internal control refers to the processes, structures and culture companies establish to identify, assess, treat and monitor risk that support the achievement of company objectives. To assist in implementing risk management, the board should ensure that management develops policies that include, at a minimum, components relating to risk oversight, risk profile, risk management, including compliance and control, and provide for assessment of the effectiveness of risk oversight and internal control and management.

A risk management system should not be applied in isolation, but rather in conjunction with other business routines and systems, for example, the planning, budgeting and reporting used to manage the company. The risk management system should take into account existing business management systems, processes and structures and should support:

- a description of the company’s risk management policy and system, including internal compliance and control, that can be made publicly available
- the board’s risk oversight function
- an assessment of the effectiveness of risk oversight and management.

Companies may already have a risk management and internal control system or process that is known by another name but which achieves the objectives of Principle 7. Companies are not asked to implement new systems, but to ensure that any system they currently have in place assists them to identify, assess, treat and monitor risk to support the achievement of their objectives.

## **What is a risk profile?**

A risk profile informs the board and management about material business risks relevant to the company. Material business risks are 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. They present opportunities and threats for financial gain or loss. Companies will often describe their risk profile in an Initial Public Offer document such as a prospectus.

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

- the health of the industry sector
- market share or size
- competition
- industrial relations
- foreign exchange and interest rates
- equity and commodity prices
- political visibility.

Companies will also have risks associated with their internal operating activities such as those emanating from:

- operational performance
- compliance
- financial control and reporting
- technology
- people and skills

- issues relating to the quality of management.

Some or all of these risks and other risks not referred to above may be relevant to a company's risk profile.

A company should advise investors of material changes to its risk profile, either through the corporate governance reporting framework, or in the directors' or chief executive officer's report in the annual report. A company may also have an obligation to inform the market of a change to its risk profile under the continuous disclosure regime, where the change is likely to have a material impact on the price or value of a company's securities.

### **What are risk oversight and management and internal control policies?**

Policies encapsulate the courses or principles of action to be adopted or proposed by the company, including key processes.

Risk oversight and management and internal control policies set out how the company discharges its 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
- risk management systems
- business policies and practices
- protection of its assets
- compliance with relevant laws, regulations, standards and best practice guidelines.

Risk management and internal control policies provide guidance on how the company:

- assesses its internal processes for determining, managing and reporting on key risk areas
- ensures that it has an effective risk management and internal control system and that material business risks to the company are reported regularly to the board
- addresses the effectiveness of the company's internal control and risk management system with management and the internal and external auditors
- assesses whether management has controls in place for unusual types of transactions and/or any potential transactions that may carry more than an acceptable degree of risk
- ensures key management, internal and external auditors and compliance staff understand and discuss the entity's control environment.

Risk management policies could include the following:

- a mission statement on risk, which might include a definition of risk such as "anything that hinders the sustainable achievement of objectives and results, including the failure to exploit opportunities", and the purpose of the policy such as "to formalise and communicate the company's approach to risk management"
- the scope of the policy
- the company's risk tolerance level
- the roles and responsibilities of; the board, any relevant board committee, management and any risk manager or other officer who assumes this duty
- other risk activities of the various groups within the company
- responsibility for external audit
- the risk assessment, measuring and reporting process
- identification and profile
- continuous monitoring.

Once the relevant risk management policy is approved by the board, the policy should be signed and dated by the chief executive officer and circulated to appropriate individuals within the company. The policy should be reviewed on a regular basis.

### **What is a material business risk?**

Material business risks have the potential to create value and protect established value. The following examples of material business risk categories are identified in Principle 7:

- operational
- environmental
- sustainability
- compliance
- strategic
- ethical conduct
- reputation or brand
- technological
- product or service quality
- human capital
- financial reporting
- market-related risks.

All companies will face some risks which have the potential to significantly or materially impact the company's performance.

### **Reporting**

The purpose of reporting is to provide meaningful information to investors about the company's risk management policies and system that could assist them in valuing the company. The following examples highlight reports that do *not* provide meaningful information to investors.

#### *Example 1*

"The company does not face any material business risks."

This example illustrates unhelpful reporting. The focus of reporting should be on a description of policies, and the robustness of the processes in place to manage risk. A company that simply states it does not have any risks has not informed investors how it came to this assessment, or what system it has in place to monitor risks on an ongoing basis.

#### *Example 2*

"The risks facing this company are well known."

As with the first example, this disclosure is unhelpful. Although the company may consider its risks to be reasonably well known, Principle 7 is actually asking for disclosures about the policies and procedures in place to manage these risks. Principle 7 also asks for an indication that management has reported to the board as to the effectiveness of the company's management of its material business risks.

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

The assurance from the chief executive officer/chief financial officer should cover financial reporting risks and the associated controls, which underpin the integrity of the company's financial reporting. Assurance in relation to financial reporting controls provides an additional level of assurance as to the integrity of the processes that support financial reporting. This assurance is not intended to suggest any

diminution of senior management accountability in relation to other aspects of a company's risk management and control system, about which the board does not require assurance.

It is implicit within the recommendation that a qualified assurance would not meet Recommendation 7.3 and therefore should be the subject of "if not, why not" reporting.

### **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 in accordance with the appropriate standards and regulations.

Effective internal control processes will generally contain some documentation of key financial reporting processes and evidence of the satisfactory operation of key internal controls over material matters. Typically, business outcomes are monitored through key performance indicators, financial and non-financial. However, events outside management's control can lead to undesirable outcomes. This would not necessarily mean that risk management is ineffective.

Assurance on effectiveness of risk management and internal control is:

- aiming to provide a reasonable but not absolute level of assurance
- no guarantee against adverse events, or losses, or more volatile outcomes arising.

### **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. The assurance should indicate if any material matter has come to the attention of the chief executive officer/chief financial officer between the reporting date and the date of signing the annual financial statements.

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.

### **What disclosures are required by Principle 7?**

As indicated in the Guide to Reporting in Principle 7, companies are asked to disclose the following:

- explanation of any departures from recommendations 7.1, 7.2 or 7.3
- 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 under Recommendation 7.1.

These disclosures should be set out in the corporate governance statement in the annual report.

### **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 risk profile
- 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.

## Sources of additional information

Companies may refer to the Group of 100 *Guide to Compliance with ASX Corporate Governance Council Principle 7 – “Recognise and Manage Risk*, which is available on the Group of 100 website at [www.group100.com.au](http://www.group100.com.au).

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

- 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](http://www.coso.org)
- *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](http://www.icaew.co.uk)
- Australian / New Zealand Standard for Risk Management (AS/NZS 4360: 1999: Risk Management) at [www.standards.com.au](http://www.standards.com.au)
- the Institute of Internal Auditors and Standards Australia publication linking AS/NZS4360 on risk management to internal control at [www.iaa.org.au](http://www.iaa.org.au).