



# Recognise and manage risk

A Guide to compliance with ASX Principle 7

# Preface

Good corporate governance practices are essential to efficient capital markets and investor confidence. Developments, both internationally and in Australia, continue to focus on these goals.

Compliance with the ASX Corporate Governance Council's *Corporate Governance Principles and Recommendations (Principles)*, which includes *Principle 7: Recognise and manage risk*, is an important element in establishing good corporate governance practices in Australia. The Group of 100 is committed to assisting in this reform process by developing guidance on implementing good practice.

This *Guide to compliance with ASX Corporate Governance Council Principle 7: Recognise and manage risk* has been prepared in association with Deloitte. It is the second edition and follows the release in August 2007 of the revised *Principles*.

The purpose of the Guide is to provide general guidance in relation to compliance with *Principle 7*. A sound and robust system of risk management and internal control designed in the context of the nature of the company and its culture is an integral part of a company's ongoing management and governance processes. The Guide does not specify or adopt a particular model or approach, however the COSO model is used as the basis of the discussion.

We believe that this Guide will serve as a valuable reference point in facilitating compliance with *Principle 7*. It is also pleasing that the ASX Corporate Governance Council has referenced this Guide in its *Supplementary Guidance to Principle 7* issued in June 2008.

**We recommend this publication to the Group of 100 members and others.**

**Tony Reeves**  
National President  
Group of 100

**Ron Loborec**  
Managing Partner  
Risk Services  
Deloitte

# Table of contents

Preface	
Executive summary	1
1. Introduction	4
2. Principle 7: Recognise and manage risk	5
3. Detailed guidance	7
Appendix 1	19
Assessing the effectiveness of the company's risk management and internal control – company layer controls	
Appendix 2	21
Illustrative wording for CEO and CFO Certifications to meet requirements of both <i>Principle 7</i> and <i>s295A Corporations Act 2001</i>	
Appendix 3	22
Key sources of information	

# Executive summary

The revised ASX Corporate Governance Council’s *Corporate Governance Principles and Recommendations* released in August 2007 (*Principles*) are the foundation of a disclosure-based ‘if not, why not?’ regime for corporate governance in Australia.

This Guide is designed to clarify and provide general guidance on some of the key issues which arise for companies when considering compliance with the revised *Principle 7: Recognise and manage risk*. The guidance covers the formal framework for risk management, breadth of controls, layers of risk management, effectiveness of management of material business risks, layers of control, levels of assurance, period of coverage, corporate reach and reporting templates.

An integral part of a company’s corporate governance is to develop appropriate risk management practices consistent with its nature and culture. It is important to communicate this appropriately to stakeholders of a company.

## Formal framework

### Question:

Should the models of the Committee of Sponsoring Organisations of the Treadway Commission (COSO) – such as the COSO Enterprise Risk Management (ERM) and COSO Internal Control models (refer to Diagrams 1 and 2) – on which both the UK and US regulatory frameworks are built – also be adopted by Australian companies?

### Guidance:

Each company should have its own documented risk management and internal control models to facilitate compliance with *Principle 7*. The COSO ERM and Internal Control models are broadly accepted examples for companies to use in developing their risk management and internal control system. These are used as the basis of the guidance in this document.

Diagram 1: COSO ERM model – Integrated Framework (Layers of risk management)

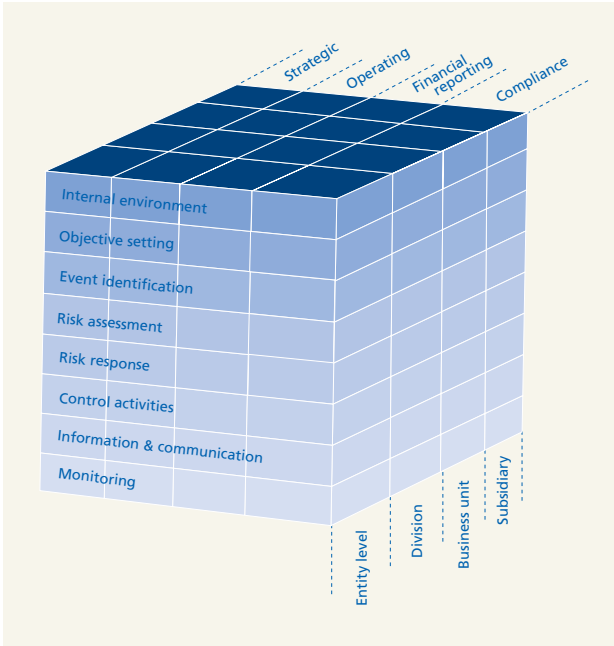
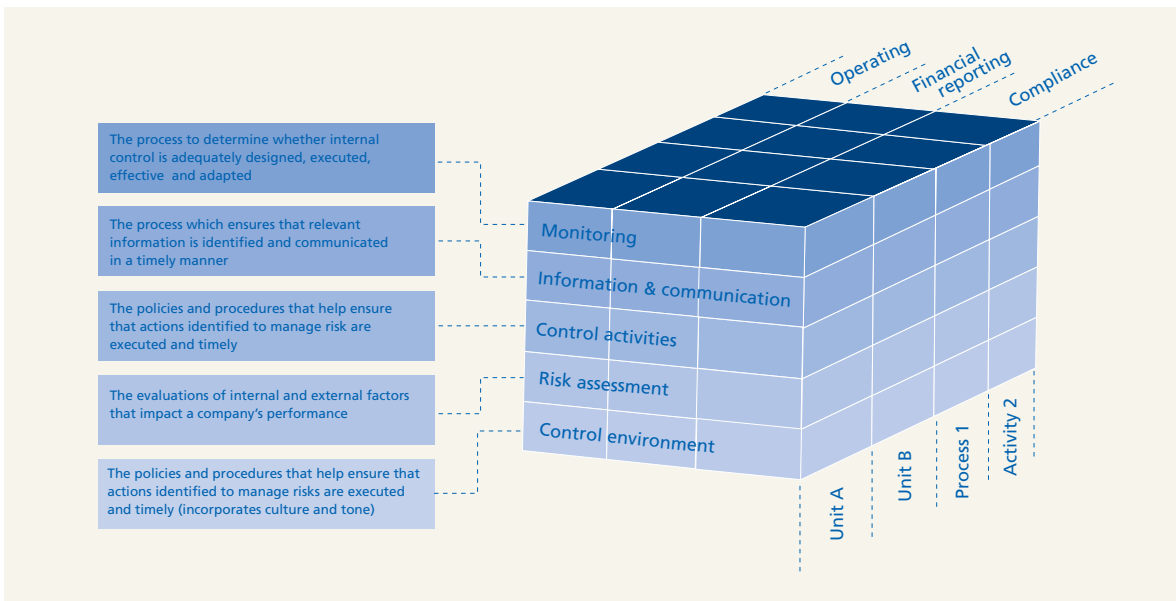


Diagram 2: COSO Internal Control model (Layers of control)



### Breadth of risks/controls

**Question:**

How should a company balance its focus on financial reporting risks and controls in respect of the CEO/CFO certification, and its focus on material business risks in respect of reporting to the Board in accordance with *Principle 7*?

**Guidance:**

The Board's oversight of risk management should encompass enterprise-wide risks including strategic, operational, financial reporting and compliance risks. The assurance provided by the CEO/CFO certification should focus on financial reporting risks and controls as well as such other risks and controls requiring assurance as specified by the Board.

### Layers of risk management

**Question:**

If the COSO ERM model is adopted, what should risk management and oversight policies include? What are the key elements to an effective risk management system?

**Guidance:**

All layers of the COSO ERM model should be implemented in a way that is appropriate to the circumstances of the company. There are a number of factors to consider when designing an effective risk management and internal control structure across all COSO ERM layers. These factors will vary from company to company.

## Effectiveness of management of material business risks

### Question:

Under *Recommendation 7.2*, what should be considered when assessing the effectiveness of the management of material business risks?

### Guidance:

Reporting on the effectiveness of managing material business risks should have regard to:

- those aspects of a risk that can be controlled through management activities or internal controls
- whether the resulting residual risk and response to that risk is acceptable having regard to the company's risk matrix.

## Layers of control

### Question:

If the COSO Internal Control model is adopted, should companies implement controls at all layers of the COSO Internal Control model and, if so, with what relative importance? How can these controls be most effectively implemented and maintained?

### Guidance:

All layers of the COSO Internal Control model should be implemented in a way that is appropriate to the circumstances of the company. There are a number of factors to consider when designing an effective internal control structure across all COSO layers and these will vary from company to company.

## Level of assurance

### Question:

What is an appropriate level of testing and what processes of testing should be used in support of providing assurance for controls?

### Guidance:

A reasonable level of assurance should be obtained from the testing of internal controls. The testing processes adopted are a matter of professional judgment and will vary from company to company. They should appropriately document all layers of the COSO Internal Control model. Testing under the Control activities layer would generally be more robust for the assurance requirements under *Recommendation 7.3* than for the reporting requirements under *Recommendation 7.2*.

## Period of coverage

### Question:

Does the period of coverage for reporting under *Recommendation 7.2* and the assurance provided under *Recommendation 7.3* include the entire reporting period up to, and including, the date of signing of the Annual Report?

### Guidance:

Companies should ensure that the reporting and assurance requirements in *Principle 7* cover the reporting period. In addition, the CEO and CFO should disclose whether any material matter has come to their attention between the reporting date and the date of signing the Annual Report.

## Corporate reach

### Question:

If an ASX-listed entity includes a variety of business structures such as subsidiaries, associates and joint ventures, which of these structures should be included in the scope of *Principle 7* compliance activities?

### Guidance:

All subsidiaries **must** be included, and all material associates and joint ventures **should** be included, within the scope of *Principle 7's* compliance activities. Where material associates and joint ventures are not included within the scope this should be disclosed.

## Reporting templates

### Question:

What disclosures and reporting are appropriate under each element of *Principle 7*?

### Guidance:

Refer the ASX Corporate Governance Council *Revised Supplementary Guidance to Principle 7*, issued June 2008, as well as Appendix 2 and the detailed guidance herein section 3.9.



# 1. Introduction

## 1.1 Background

In March 2003, the ASX Corporate Governance Council (CGC) issued *Principles of Good Corporate Governance and Best Practice Recommendations*. After three years of practical experience, the CGC conducted its first review to remove areas of regulatory overlap with the *Corporations Act 2001* and accounting standards, and to provide further assistance to companies and investors by clarifying the application of certain principles.

In August 2007, the revised *Corporate Governance Principles and Recommendations (Principles)* were issued. The revised *Principles* continue to adopt the non-prescriptive 'if not, why not' approach towards disclosure of corporate governance practices. One of these *Principles* is *Principle 7: Recognise and manage risk*.

The key changes to the *Principles* include:

- removing the term 'best practice'. This is to reinforce that there is no singular best way to structure and conduct corporate governance. Corporate governance needs to be refined to the nature and culture of each company
- reducing the number of *Principles* from 10 to 8 and the number of *Recommendations* from 28 to 26. *Principle 8* has been combined with *Principles 1* and *2*, and *Principle 10* has been included in *Principles 3* and *7*
- expanding the scope of *Principle 7* to require companies to report on whether 'material business risks' have been managed effectively.

The ASX Listing Rules require listed entities to include a statement disclosing the extent to which they have followed the recommendations of the CGC during the reporting period. Where companies have not followed all the recommendations, they must identify the recommendations that have not been followed and give reasons for not following them (ASX Listing Rule 4.10.3).

The revised *Principles* apply for financial years beginning on or after 1 January 2008, that is a company having a 30 June balance date must comply with the revised *Principles* for the year ending 30 June 2009.

## 1.2 Objective of this Guide

The objective of this Guide is to clarify and provide general guidance in a number of areas relating to compliance with the revised *Principle 7*. Implementation of the guidance may require judgment to be exercised in ensuring compliance with the recommendations.

The Group of 100 considers that compliance with this Guide will facilitate the establishment of a sound system of risk oversight and management and internal control. This Guide is based on the premise that a company's Board of directors has adopted a risk-based approach to establishing a sound system of internal control which it reviews for effectiveness. This process should form part of the company's normal management and governance processes and should not be treated as an exercise that is undertaken merely to meet regulatory requirements.

In preparing this Guide consideration has been given to ensuring consistency with (and minimising duplication for those companies also having to comply with) other similar internal control frameworks, such as the Combined Code in the United Kingdom and the Sarbanes-Oxley regime in the United States.



## 2. Principle 7: Recognise and manage risk

### 2.1 What is Principle 7: Recognise and manage risk?

#### Principle 7: Recognise and manage risk

Companies should establish a sound system of risk oversight and management and internal control.<sup>29</sup>

Risk management is the culture, processes and structures that are directed towards taking advantage of potential opportunities while managing potential adverse effects.<sup>30</sup>

Risk management should be designed to:

- identify, assess, monitor and manage risk
- identify material changes to the company's risk profile.<sup>31</sup>

Risk management can enhance the environment for identifying and capitalising on opportunities to create value and protect established value.

The company should address risks that could have a material impact on its business (material business risks), as identified by the company's risk management system. The board should regularly review and approve the risk management and oversight policies.

#### Recommendation 7.1:

Companies should establish policies for the oversight and management of material business risks and disclose a summary of those policies.<sup>32</sup>

#### 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.

#### 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.

#### Recommendation 7.4:

Companies should provide the information indicated in the Guide to reporting on Principle 7.

An extract from ASX Corporate Governance Principles and Recommendations, 2nd Edition, 2007<sup>1</sup>



## 2.2 Key questions surrounding Principle 7: Recognise and manage risk

The key questions that have been identified by companies seeking to achieve compliance with *Principle 7* are as follows:

### Formal framework:

Should the models of the Committee of Sponsoring Organisations of the Treadway Commission (COSO) such as the COSO Enterprise Risk Management (ERM) and COSO Internal Control models – on which both the UK and US regulatory frameworks are built – also be adopted by Australian companies?

### Breadth of risks/controls:

How should a company balance its focus on financial reporting risks and controls in respect of the CEO/CFO certification, and its focus on material business risks in respect of reporting to the Board in accordance with *Principle 7*?

### Layers of risk management:

If the COSO ERM model is adopted, what should risk management and oversight policies include? What are the key elements to an effective risk management system?

### Effectiveness of management of material business risks:

Under *Recommendation 7.2*, what should be considered when assessing the effectiveness of the management of material business risks?

### Layers of controls:

If the COSO Internal Control model is adopted, should companies implement controls at all layers of the COSO Internal Control model and, if so, with what relative importance? How can these controls be most effectively implemented and maintained?

### Level of assurance for controls:

What is an appropriate level of testing, and what processes of testing should be used in support of providing assurance for controls?

### Period of coverage:

Does the period of coverage for reporting under *Recommendation 7.2* and the assurance provided under *Recommendation 7.3* include the entire reporting period up to, and including, the date of signing of the Annual Report?

### Corporate reach:

If an ASX-listed entity includes a variety of business structures such as subsidiaries, associates and joint ventures, which of these structures should be included in the scope of *Principle 7* compliance activities?

### Reporting templates:

What disclosures and reporting are appropriate under each element of *Principle 7*?

## 3. Detailed guidance

### 3.1 Formal framework

#### Question:

Should the models of the Committee of Sponsoring Organisations of the Treadway Commission (COSO) such as the COSO Enterprise Risk Management (ERM) and COSO Internal Control models – on which both the UK and US regulatory frameworks are built – also be adopted by Australian companies?

The *Principles* refer to a range of guidance upon which to base a sound system of risk oversight and management and internal control. These include the COSO models (ERM and Internal Control) and the *Australian/New Zealand Standard for Risk Management AS/NZS 4360:2004*. In addition, a new global risk management standard, *ISO 31000: Risk Management – Principles and guidelines on implementation*, is currently under development.

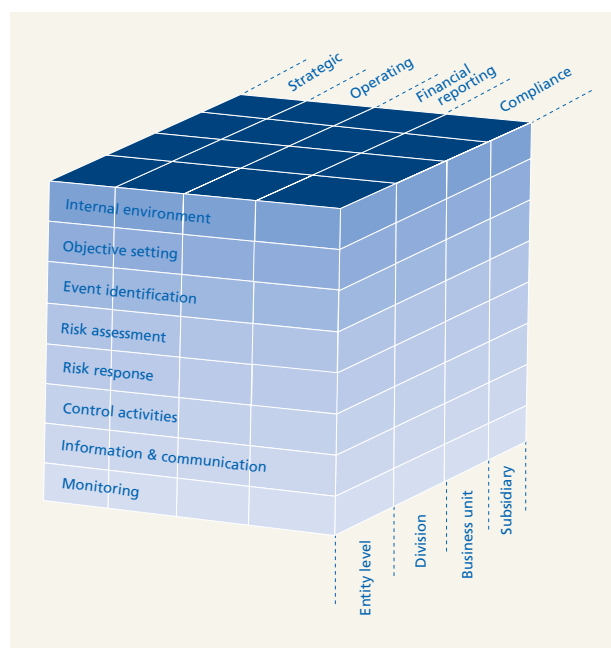
In 1992, the Committee of Sponsoring Organisations of the Treadway Commission developed a formal framework for implementing and maintaining a system of risk management and internal control, known as the COSO Internal Control model.

In 2006, COSO released the Enterprise Risk Management – integrated framework (COSO ERM model), which expands on internal control, providing a more robust and extensive focus on the broader subject of enterprise risk management.

A diagrammatic representation of these models is shown in Diagram 1 and Diagram 2, and further information is available at [www.coso.org](http://www.coso.org).

The COSO ERM model adopts a holistic view of risk management within an entity and covers the four key categories (strategic, operations, reporting, and compliance) across the entity and at each division, business unit and subsidiary. At the same time, the framework focuses on eight inter-related risk management components: internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring.

Diagram 1: COSO ERM model – Integrated Framework (Layers of risk management)



1 Sourced from COSO's *Enterprise Risk Management – Integrated Framework Executive* September 2004.

Enterprise risk management encompasses<sup>1</sup>:

- **aligning risk appetite and strategy –**  
Management considers the entity's risk appetite in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks
- **enhancing risk response decisions –**  
Enterprise risk management provides the rigour to identify and select among alternative risk responses – risk avoidance, reduction, sharing, and acceptance
- **reducing operational surprises and losses –**  
Entities gain enhanced capability to identify potential events and establish responses, reducing surprises and associated costs or losses
- **identifying and managing multiple and cross-enterprise risks –**  
Every enterprise faces a myriad of risks affecting different parts of the organisation, and enterprise risk management facilitates effective response to the interrelated impacts, and integrated responses to multiple risks
- **seizing opportunities –**  
By considering a full range of potential events, management is positioned to identify and proactively realise opportunities
- **improving deployment of capital –**  
Obtaining robust risk information allows management to effectively assess overall capital needs and enhance capital allocation.

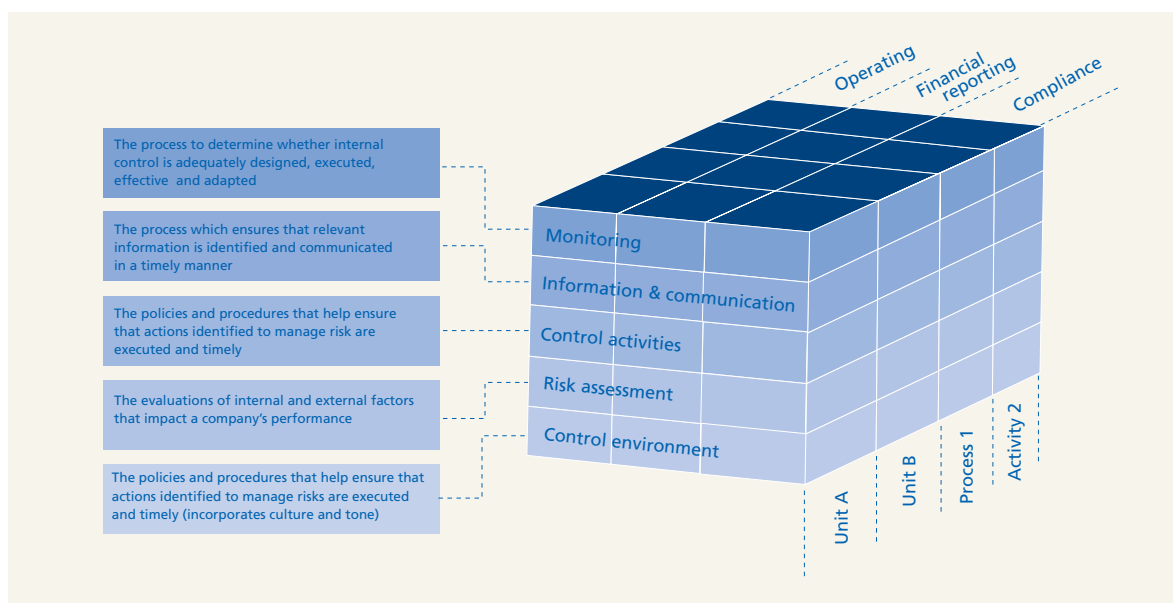
The COSO Internal Control model is recognised explicitly in the Sarbanes-Oxley internal control regime and implicitly in the UK Combined Code internal control regime. The COSO Internal Control model provides further depth and clarification to the control activities layer within the COSO ERM model.

The Group of 100 recognises that the COSO ERM model and *AS/NZS Risk Management 4360:2004* are considered the preferred global frameworks for enterprise risk management and internal control. The Group of 100 also recognises that because of the diversity due to factors such as their size, complexity and culture, companies should have flexibility to develop a risk management and internal control model suitable to their circumstances but, in so doing, should have regard to the recognised COSO ERM and Internal Control models.

**Guidance:**

Each company should have its own documented risk management and internal control models to facilitate compliance with *Principle 7*. The COSO ERM and Internal Control models are broadly accepted examples for companies to use in developing their risk management and internal control system. These are used as the basis of the guidance in this document.

Diagram 2: COSO Internal Control model (Layers of control)



1 Sourced from *COSO's Enterprise Risk Management – Integrated Framework Executive* September 2004.

### 3.2 Breadth of risks/controls

#### Question:

How should a company balance its focus on financial reporting risks and controls in respect of the CEO/CFO certification, and its focus on material business risks in respect of reporting to the Board in accordance with Principle 7?

*Recommendation 7.1* of the revised *Principle 7* has clarified the scope of risks to be considered by adopting the concept of 'material business risks'. That is, a holistic approach should be adopted when recognising and managing risk.

The COSO ERM model views a company's objectives in four key categories, namely:

- strategic
- operations
- financial reporting
- compliance.

These categories are consistent with the guidelines for material business risks set out in revised *Principle 7*.

In this context:

- 'material' should be interpreted by reference to accounting standards on materiality and have regard to both quantitative and qualitative factors
- 'business' requires a risk to have some connection with the four categories outlined above
- material business risks should be considered at a whole-of-company level
- material business risks are a subset of the company's entire risk profile
- 'non-material' business risks should not necessarily be ignored as in future years they may become material business risks, or have a significant impact when taken in conjunction with other risks. Management may still recognise and manage such risks in a formalised manner but not necessarily report to the Board on the effectiveness of their management.

The COSO Internal Control model recognises that controls can be established for three of the four categories: operations, financial reporting and compliance. By implication, strategic risks are a function of management decisions as to where to operate and therefore impact the risk profile or inherent risks of a company, but do not necessarily have directly attributed controls.

When a company is establishing and implementing its approach to risk management, it should consider the COSO categories of risk and control in determining its material business risks.

*Recommendation 7.2* requires management to design and implement the risk management and internal control system to manage the company's material business risks and to report to the Board on whether those risks are being managed effectively. This involves appropriate assignment of accountabilities for managing the material business risks identified under *Recommendation 7.1*.

The CEO would normally have joint responsibility for all material business risks along with, for example, the COO for operational risks, the CFO for financial reporting risks, the Company Secretary/Legal Counsel for compliance risks, the CIO for information technology risks, and the Director of HR for human capital risks, etc.

*Recommendation 7.3* relates only to financial reporting risks and the integrity of the financial statements by underpinning the CEO/CFO declaration under s295A of the *Corporations Act 2001*. The specific requirement for the Board to seek 'assurance' from the CEO/CFO in this area recognises the importance of financial statements and broadly aligns with international regimes.

(Note: Sarbanes-Oxley focuses strictly on risks and controls in the category of financial reporting, whereas the UK Combined Code covers all COSO categories of risk and control.)

It is also important to differentiate that *Recommendation 7.2* requires only **reporting** on the effectiveness of managing material business risk while *Recommendation 7.3* requires **assurance**. However, it is acknowledged that the Board may seek additional assurance or certification pertaining to other areas of material business risk. In these situations the CEO and CFO certifications will need to clearly state that they relate to controls over the integrity of financial reporting and identify those additional risks and controls as communicated by the Board (refer Appendix 2). The form of this communication will depend on how the Board manages the relationship with management.

#### Guidance:

The Board's oversight of risk management should encompass enterprise-wide risks including strategic, operational, financial reporting and compliance risks. The assurance provided by the CEO/CFO certification should focus on financial reporting risks and controls as well as such other risks and controls requiring assurance as specified by the Board.

### 3.3 Layers of risk management

#### Question:

If the COSO ERM model is adopted, what should risk management and oversight policies include? What are the key elements to an effective risk management system?

The revised *Principle 7* requires the Board to review annually:

- the policies for the oversight and risk management of material business risks
- the effectiveness of the system of risk management and internal control.

Underpinning both this policy and the system is a risk management framework. It is important for companies to have due regard to the ERM framework in building effective programs for identifying, measuring, prioritising and responding to material business risks.

As shown in Diagram 1 on page 7, the eight inter-related components in the COSO ERM model each provide a different element of the overall risk management framework. While different degrees of emphasis exist between the COSO ERM components, there is no express ranking of the relative importance of each of these components.

Identifying and managing whole-of-company and cross-divisional risks should be a key focus for companies. This allows companies to have a portfolio view of their risks and contributes towards breaking down silos within the company.

While recognising that each 'higher' component precedes the underlying components – reflecting the 'top-down' nature of risk management – the Group of 100 notes that, for the COSO ERM model to operate effectively, all components need to co-exist and operate collectively.

In designing an effective risk management system consideration should be given to:

- the company's objectives
- the company's internal organisation
- the environment in which the company operates
- the degree of risk willing to be accepted (the company's risk appetite)
- the company's culture
- the cost-benefit issues.

Such factors are continually evolving and consequently the design of the risk management system should be regularly evaluated.

A risk management policy should outline the company's approach to managing risk including the description of responsibilities and the frequency of actions. It should also set out the process for risk management within the company including, but not limited to, identifying, assessing, responding to and monitoring of risks.

The following – non-exhaustive – listing of components of an effective risk management system provides examples to consider depending on a company's circumstances:

- risk management policy
- risk management plan
- risk management framework (standards and guidance)
- risk matrix (to facilitate rating and prioritisation of residual risks post evaluation of control effectiveness)
- risk registers
- action plans (for treatment of risks)
- communication plans (to educate and sustain risk management)
- incident reporting
- control self-assessment
- risk response (including assurance plan and reporting to the executive and Board requirements)
- benchmarking (to assist in determining how risk mature the company is, and wants to be, to ensure a fit-for-purpose risk management system).

Table 1: COSO ERM model: Examples of components by layer

COSO ERM layer	Example components
Internal environment	Code of conduct Corporate culture/values/tone/commitment
Objective setting	Strategic business plans and linkages to internal audit program
Event identification	Workshops from strategic planning process Incident/events reporting system
Risk assessment	Risk-control matrices and linkages to internal audit program
Risk response	Action plans Risk Management Committee to review responses to risks
Control activities	Policies and procedures manuals Process flowcharts Inventory of controls including accountabilities Manual and automated controls Mix of preventative and detective/monitoring controls Information technology controls
Information and communication	Risk profiles/registers Appropriate information systems Company reporting guidelines Feedback/whistleblower channels
Monitoring	Specific Board and/or senior management committees reporting through to the Board e.g. Risk Management Committee Internal audit function Control self-assessments

The Group of 100 considers that appropriate and regular corporate profiling and/or training is necessary to reinforce and refresh the risk management and internal controls systems within a company.

**Guidance:**  
All layers of the COSO ERM model should be implemented in a way that is appropriate to the circumstances of the company. There are a number of factors to consider when designing an effective risk management and internal control structure across all COSO ERM layers. These factors will vary from company to company.

### 3.4 Effectiveness of the management of material business risks

**Question:**

Under *Recommendation 7.2*, what should be considered when assessing the effectiveness of the management of material business risks?

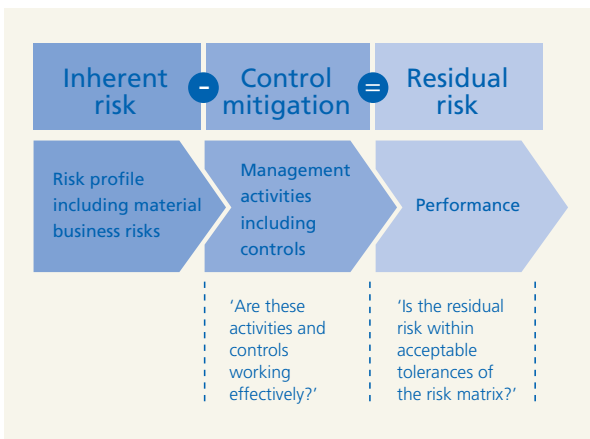
Risk management is not about eliminating risk. Some risks cannot be managed and some may not be cost-effective to manage.

However, the resulting residual risk may indicate a need to further tighten or relax controls in order to bring the residual risk within an acceptable level of risk tolerance.

Consequently, the management of material business risks should have regard to the effectiveness to which management applies controls and other activities to reduce inherent risk to an acceptable residual risk defined within the company's risk matrix.

The following diagram may assist:

Diagram 3: Effectiveness of management of risk



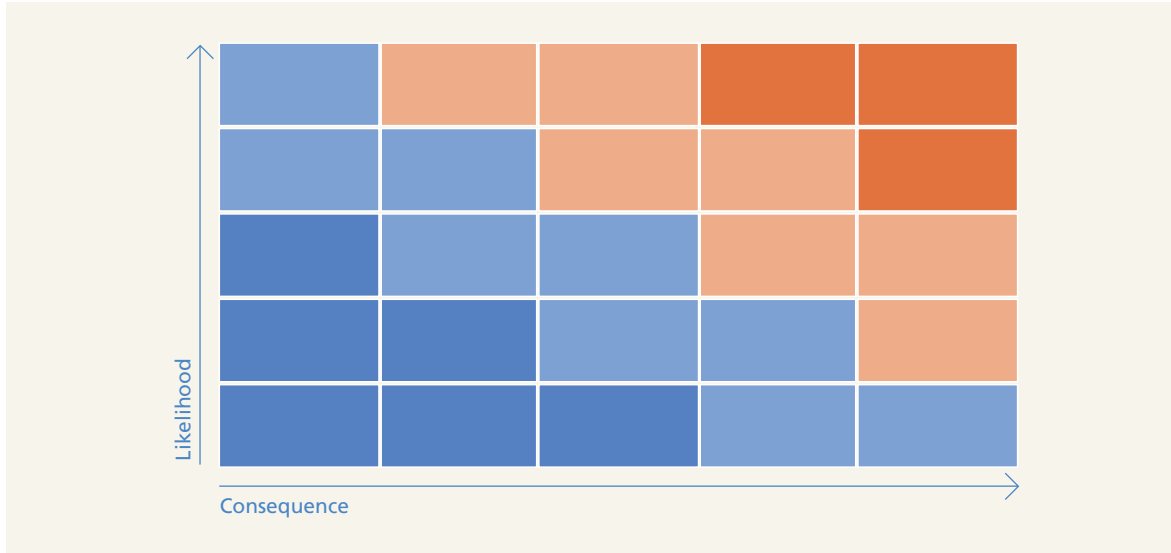
To evaluate controls that mitigate material business risk, management should make an appropriate assessment at least annually. This can be by a control self-assessment approach which may, or may not, be supported by specific control testing. This evaluation should have regard to the COSO Internal Control model (see sections 3.5 'Layers of control' and 3.6 'Level of assurance for controls' following).

Internal Audit may be utilised to provide further independent comfort to the Board and management on the effectiveness of controls and activities. However management should not solely rely on Internal Audit to provide this assurance to the Board.

A risk matrix, like that shown in Diagram 4 following, will assist in defining whether the resulting residual risk is acceptable.



Diagram 4: Determining the acceptability of residual risk



Management, in consultation with the Board, should determine what is an acceptable level of risk and what is not. For example, management may determine that any material business risks that fall within the red area are not acceptable and require a specific risk response in order to be reduced to an acceptable level. Disclosure of this is not specifically required under *Principle 7* but consideration should be given to other continuous disclosure requirements.

**Guidance:**  
Reporting on the effectiveness of managing material business risks should have regard to:

- those aspects of a risk that can be controlled through management activities or internal controls
- whether the resulting residual risk, and response to that risk, is acceptable having regard to the company's risk matrix.

Under *Recommendation 7.2* management is required to report to the Board on these risks. However the Board, at its discretion, may specifically request a sign-off from the CEO and other relevant executives on some or all of the material business risks.



### 3.5 Layers of control

#### Question:

If the COSO Internal Control model is adopted, should companies implement controls at all layers of the COSO Internal Control model and, if so, with what relative importance? How can these controls be most effectively implemented and maintained?

There are five 'layers' of control in the COSO Internal Control model, each providing a different element of the overall internal controls framework. These layers are the control environment, risk assessment, control activities, information and communication, and monitoring (see Diagram 2, page 8). Both Sarbanes-Oxley and the UK Combined Code refer to the need for all five COSO layers to be addressed in a company's system of risk management and internal control.

While different degrees of emphasis exist between COSO layers in these frameworks, there is no express distinction of importance between layers.

While recognising that each 'higher' layer is dependent upon its underlying layers, the Group of 100 notes that for the COSO Internal Control model to operate effectively all layers need to co-exist and operate collectively.

The process of effectively implementing and maintaining controls for each of the COSO layers will vary from company to company. In designing a control structure consideration should be given to:

- the company's objectives
- the company's internal organisation
- the environment in which the company operates
- the degree of risk willing to be accepted (the company's risk appetite)
- the company's culture
- the cost-benefit issues.

Such factors are continually evolving and consequently the design of the control structure should be regularly evaluated.

The table below provides a non-exhaustive set of examples of how, depending on a company's circumstances, controls can be effectively implemented and maintained over the five COSO layers. Some of these examples are also relevant for the COSO ERM model described in section 3.3. Appendix 1, page 19, contains a further illustrative template/checklist.

The Group of 100 considers that appropriate and regular corporate profiling and/or training is necessary to reinforce and refresh the internal controls in place for each COSO internal controls layer within a company.

#### Guidance:

All layers of the COSO Internal Control model should be implemented in a way that is appropriate to the circumstances of the company. There are a number of factors to consider when designing an effective internal control structure across all COSO layers and these will vary from company to company.

Table 2: COSO Internal Control model: Examples of control by layer

COSO Internal Control layer	Examples of control
Control environment	Code of conduct Corporate culture/values/tone/commitment External regulatory environments
Risk assessment	Utilise COSO ERM or AS/NZS 4360 Risk registers Risk-control matrices and linkages to internal audit program
Control activities	Policies and procedures manuals Process flowcharts Inventory of controls including accountabilities Manual and automated controls Mix of preventative and detective/monitoring controls Information technology controls
Information and communication	Appropriate information systems Company reporting guidelines Feedback/whistleblower channels
Monitoring	Specific Board and/or senior management committees reporting through to the Board e.g. Board Audit Committee Internal audit function Control self-assessments

### 3.6 Level of assurance for controls

#### Question:

What is an appropriate level of testing and what processes of testing should be used in support of providing assurance for controls?

*Principle 7* requires the testing of controls for:

- assessing the effectiveness of managing material business risks under *Recommendation 7.2* (See section 3.4 Effectiveness of management of material business risks above)
- providing the necessary assurance for the annual financial reporting control certification by the CEO and CFO.

The *Revised Supplementary Guidance to Principle 7* (CGC, June 2008) clearly sets out that a 'reasonable but not absolute level of assurance' is required to be provided to the Board.

This would cover all five layers of the COSO Internal Control model noted in section 3.5 Layers of control.

Four of the five layers of the COSO Internal Control model – control environment, risk assessment, information and communication, and monitoring – should be considered and evidenced using an appropriate checklist. A brief example is provided in Appendix 1.

For the Control activities layer the following is noted:

- a. *Recommendation 7.3* – given the specific 'assurance' requirement for financial reporting controls this will often involve documentation of the:
  - key reporting processes such as revenue, expenditure, payroll, financial close, etc
  - evidence of the effectiveness of key controls including:
    - design effectiveness: Does the control exist? Is the control structured appropriately to mitigate the risk?
    - operational effectiveness: Is the control working as intended?
- b. *Recommendation 7.2* – the evidence of controls working to assist in the evaluation of the effectiveness of material business risks may be produced to the same standard as outlined above. As an alternative, the following level of effort may also be appropriate:
  - a regular program of internal audits linked to the risk control matrix
  - periodic and comprehensive control self-assessments, with independent follow-up

- specific and specialised assurance activities in high risk areas appropriate to the company (covering areas such as information security and treasury).

In arriving at any conclusions on the testing of internal controls the following factors should be taken into account:

- testing is not performed throughout the period
- testing evidence is often persuasive rather than conclusive
- tests performed are on a sample basis of the complete population.

All testing and conclusions reached should be fully documented.

The following Australian standards may provide useful additional guidance on these matters:

- *Australian Auditing Standard 810 – Special Purpose Reports on the Effectiveness of Control Procedures*
- *Australian Standard on Assurance Engagements 3000 – Assurance Engagements Other than Audits or Reviews of Historical Financial Information.*

#### Guidance:

A reasonable level of assurance should be obtained from testing of internal controls. Testing processes adopted are a matter of professional judgment and will vary from company to company. They should appropriately document all layers of the COSO Internal Control model. Testing under the Control activities layer would generally be more robust for the assurance requirements under *Recommendation 7.3* than for the reporting requirements under *Recommendation 7.2*.

### 3.7 Period of coverage

**Question:**

Does the period of coverage for reporting under *Recommendation 7.2* and the assurance provided under *Recommendation 7.3* include the entire reporting period up to and including the date of signing the Annual Report?

Yes. It is explicit in the ASX Listing Rules that a company's statement of compliance in relation to the *Principles* in the Annual Report must cover the reporting period and as outlined in the *Revised Supplementary Guidance to Principle 7 (June 2008)*, for financial reporting controls.

The ASX Listing Rules also require that statements in the Annual Report be current as at a date within six weeks of when the Annual Report is sent to shareholders. In nearly all cases this will be more than six weeks after balance sheet date.

This implies that, in addition to the certification of controls for the reporting period (ie. the financial year), a degree of certification is required for the period from the end of the reporting period to the signing of the controls certification in the Annual Report.

Given the timing practicalities of this certification, the Group of 100 considers that, in addition to the statements made for the reporting period, to be consistent with ASX Listing Rules it would be appropriate to make reference to any material matter coming to the attention of the CEO or CFO in the intervening subsequent events period (refer Appendix 2).

These requirements differ from the Sarbanes-Oxley regime which requires certification at a point in time.

**Guidance:**

Companies should ensure that the reporting and assurance requirements in *Principle 7* cover the reporting period. In addition, the CEO and CFO should represent whether any material matter has come to their attention between the reporting date and the date of signing the Annual Report.

### 3.8 Corporate reach

**Question:**

If an ASX-listed entity includes a variety of business structures such as subsidiaries, associates and joint ventures, which of these structures should be included in the scope of *Principle 7* compliance activities?

The revised *Principle 7* includes a reference to the inclusion of subsidiaries, associates and joint ventures as defined in *AASB 128 Investments in Associates*.

This differs from the Sarbanes-Oxley requirements where only consolidated subsidiaries and the parent company are required to be included in the scope of coverage.

The UK Combined Code provides that subsidiaries are included within its scope but the inclusion of material joint ventures and associates is not mandatory. However where material joint ventures and associates are not included, disclosure of this fact is required by the Combined Code.

In light of the importance in Australia of associates and joint ventures, the Group of 100 considers that the UK disclosure approach is appropriate good practice. Guidance on the application of materiality is included in *AASB 1031 Materiality*.

**Guidance:**

All subsidiaries must be included, and all material associates and joint ventures should be included, within the scope of *Principle 7's* compliance activities. Where material associates and joint ventures are not included within the scope this should be disclosed.

### 3.9 Reporting templates

#### Question:

What disclosures and reporting are appropriate under each element of *Principle 7*?

*Principle 7* requires the following reporting and disclosures:

1. a summary of the policies established for the oversight and management of material business risks should be on the company's website
2. a report from management to the Board on the effectiveness of:
  - a. managing material business risks
  - b. the risk management and internal control system
3. an assurance declaration from the CEO/CFO to the Board relating to financial reporting controls
4. disclosure in the corporate governance statement:
  - a. that the Board has received the above:
    - i. effectiveness reports on the risk management and internal control system and material business risks from management
    - ii. assurance declaration from the CEO/CFO
  - b. any departures from the requirements set out in *Principle 7*.

Consistent with the philosophy of open disclosure and an 'if not, why not' regime, the CGC does not prescribe the content, format or style of the Annual Report or website disclosures or CEO/CFO certifications required under the *Principles*.

#### Requirements 1 and 4

In respect of requirements 1 and 4 (above), the CGC has provided further guidance, including both 'helpful' and 'unhelpful' examples of disclosure, in the *Revised Supplementary Guidance to Principle 7 (June 2008)*.

To support this, the Group of 100 suggests disclosures on the following items could be made on a company's website or in its Corporate Governance Statement:

- an overview and details of the key elements of the company's risk management and internal control model (or reference to the COSO model if adopted)
- the roles and responsibilities of the Board and management in the model
- information and overview but no detail on the key risk exposures of the company.

#### Requirement 2

In respect of reporting from management to the Board, it is important to note that this reporting should be occurring throughout the year with a summary report at year-end.

Some reporting documents and suggested content are set out below:

- material business risk profiles:
  - provided throughout the year at a level of detail and frequency consistent with the residual risk rating (ie higher the rating the more detail and more frequent reporting)
  - contents may include:
    - appropriate description of risk
    - responsibility
    - management control rating
    - overall residual risk rating along with consequence and likelihood elements
    - risk direction
    - speed of onset of a risk occurrence
    - details of interdependent or related risks
    - context of risk (why is this important to the company)
    - details of controls/risk response
    - details of any management assurance
    - details of action plans
    - log of risk occurrences
- annual risk summary report:
  - provided at the same time the annual report is considered and approved
  - outlines the process followed throughout year covering:
    - review of risk policy
    - review of risk framework
    - review of risk matrix
    - summary of process and results of risks identification and rating process
    - summary of material business risk profiles
  - may contain statement (if Board requests) from CEO and/or Group Risk/other executives as to the risk management and internal control system and the managing of material business risk. An adaptation of the illustration in Appendix 2 may be suitable
- internal audit report:
  - if requested by the Board, the results of any internal audit activity additional to the above throughout the year.

#### Requirement 3

In respect of requirement 3, the CEO/CFO certification can be combined with the s295A *Corporations Act 2001* requirement. Appendix 2 provides an example of this joint certification.

#### Guidance:

Refer the ASX Corporate Governance Council *Revised Supplementary Guidance to Principle 7*, issued June 2008, as well as Appendix 2 and the detailed guidance above.



# Appendix 1

## Assessing the effectiveness of the company's risk management and internal control – company layer controls.

To assist the CEO and CFO in discharging their responsibility for their *Principle 7* certification, the template on the following page may be useful for documenting the company layer controls within the COSO Internal Control model.

The template and issues to consider should be adapted to the company's particular circumstances, such as for multiple locations.

This guidance is based on the criteria set out in the COSO Internal Control model and the guidance to directors issued by The Institute of Chartered Accountants in England and Wales.

COSO criteria	Specific controls identified	How are controls evaluated?	Assessment of controls (Scale: Weak = 1; Strong =5)
Control environment	<ol style="list-style-type: none"> <li>1. Are the directors and management committed to leadership by example?</li> <li>2. Is the organisational structure defined clearly such that employees know what is expected of them and so as to ensure that decisions are made and actions taken by the appropriate people?</li> <li>3. Has the Board established clear strategies for addressing the significant risks that have been identified and have policies been established on how to manage these risks?</li> <li>4. Do employees have the knowledge, skills and tools to support the achievement of the company's objectives and to effectively manage its risks?</li> <li>5. Are controls adjusted as new risks or operational deficiencies are identified?</li> <li>6. Is there a professional approach to financial reporting in compliance with Australian Accounting Standards?</li> <li>7. Does a code of conduct/ethical behaviour exist and known by executives and staff?</li> <li>8. Is the company's culture supportive of an appropriate risk and control culture?</li> </ol>		
Risk assessment	<ol style="list-style-type: none"> <li>1. Are the company's objectives clear?</li> <li>2. Are significant operational, financial and compliance risks assessed on an ongoing basis?</li> <li>3. Are the risks which are acceptable to the Board clearly understood by management and employees?</li> </ol>		
Information and communication	<ol style="list-style-type: none"> <li>1. Are management and the Board provided with ongoing, up-to-date, relevant and reliable financial and other information on the company's progress against its business objectives in order to identify developments which require their intervention?</li> <li>2. Do business continuity/disaster recovery plans exist for IT monitoring and reporting systems?</li> <li>3. Is there an established system of communication for individuals to report suspected breaches of laws or regulations (whistleblower)?</li> </ol>		
Monitoring controls	<ol style="list-style-type: none"> <li>1. Are there established processes to provide the Board with ongoing assurance that there are appropriate control procedures in place for the company/group's financially significant business activities, and that these procedures are being followed?</li> <li>2. Are changes in the business or its environment which may require changes to the system of internal control identified?</li> <li>3. Are there procedures to ensure that appropriate corrective action is taken in response to the risk and control assessments?</li> <li>4. Is there communication to the Board on the effectiveness of ongoing monitoring?</li> <li>5. Does an independent internal audit function exist (in-sourced, co-sourced or out-sourced)?</li> </ol>		

# Appendix 2

## Illustrative wording for CEO and CFO Certifications to meet requirements of both Principle 7 and s295A Corporations Act 2001.

### Statement to the Board of Directors of [company]

The Chief Executive Officer and Chief Financial Officer state that:

- a. with regard to the integrity of the financial statements of [company] for the year ended [reporting date] that:
  - i. the financial records of the company have been properly maintained in accordance with s286 of the *Corporations Act 2001*
  - ii. the financial statements and notes thereto comply with Australian Accounting Standards in all material respects
  - iii. the financial statements and notes thereto give a true and fair view, in all material respects, of the financial position and performance of the company and consolidated entity
  - iv. in our opinion, the financial statements and notes thereto are in accordance with the *Corporations Act 2001*
  - v. in our opinion, there are reasonable grounds to believe that the company will be able to pay its debts as and when they become due and payable.
- b. with regard to risk management and internal control systems of [company] for the year ended [reporting date]:
  - i. the statements made in (a) above regarding the integrity of the financial statements and notes thereto is founded on a sound system of risk management and internal control which, in all material respects, implements the policies adopted by the Board of directors
  - ii. the risk management and internal control systems to the extent they relate to financial reporting [specify other, if any] are operating effectively, in all material respects, based on the [risk management model adopted by the company]
  - iii. nothing has come to our attention since [reporting date] that would indicate any material change to the statements in (i) and (ii) above.

### Chief Executive Officer

[Same date as Directors' Declaration]

### Chief Financial Officer

[Same date as Directors' Declaration]

# Appendix 3

## Key sources of information

1. ASX Corporate Governance Council: [www.asx.com.au/corporategovernance](http://www.asx.com.au/corporategovernance)
2. Deloitte: [www.deloitte.com/au/corporate\\_governance](http://www.deloitte.com/au/corporate_governance)
3. Group of 100: [www.group100.com.au](http://www.group100.com.au)
4. Institute of Internal Auditors: Guidance on implementing *Principle 7: 'Recognise and manage risk' of the 2007 Edition of the ASX Corporate Governance Principles and Recommendations*. [www.iaa.org.au](http://www.iaa.org.au)
5. COSO Internal Controls and ERM models: [www.coso.org](http://www.coso.org)
6. Sarbanes-Oxley Act of 2002 (US): [www.sec.gov/about/laws.shtml](http://www.sec.gov/about/laws.shtml)
7. American Institute of Certified Public Accountants (AICPA): [www.aicpa.org/sarbanes/index.asp](http://www.aicpa.org/sarbanes/index.asp)
8. UK Financial Reporting Council for Revised Turnbull Guidance (Oct 2005) and related corporate governance material: [www.frc.org.uk/corporate/internalcontrol.cfm](http://www.frc.org.uk/corporate/internalcontrol.cfm)
9. Institute of Chartered Accountants in England and Wales for UK Corporate Governance Codes and Reports: [www.icaew.com/index.cfm?route=159066](http://www.icaew.com/index.cfm?route=159066)
10. AS/NZS 4360:2004 Risk Management: [www.standards.org.au](http://www.standards.org.au)

## Endnote

<sup>1</sup> Form of Copyright Notice for *Corporate Governance Principles and Recommendations 2nd Edition*

© Copyright 2007 ASX Corporate Governance Council

Association of Superannuation Funds of Australia Ltd, ACN 002 786 290, Australian Council of Superannuation Investors, Australian Financial Markets Association Limited ACN 119 827 904, Australian Institute of Company Directors ACN 008 484 197, Australian Institute of Superannuation Trustees ACN 123 284 275, Australasian Investor Relations Association Limited ACN 095 554 153, Australian Shareholders' Association Limited ACN 000 625 669, ASX Limited ABN 98 008 624 691 trading as Australian Securities Exchange, Business Council of Australia ACN 008 483 216, Chartered Secretaries Australia Ltd ACN 008 615 950, CPA Australia Ltd ACN 008 392 452, Financial Services Institute of Australasia ACN 066 027 389, Group of 100 Inc, The Institute of Actuaries of Australia ACN 000 423 656, The Institute of Chartered Accountants in Australia ARBN 084 642 571, The Institute of Internal Auditors - Australia ACN 001 797 557, Investment and Financial Services Association Limited ACN 080 744 163, Law Council of Australia Limited ACN 005 260 622, National Institute of Accountants ACN 004 130 643, Property Council of Australia Limited ACN 008 474 422, Securities & Derivatives Industry Association Limited ACN 089 767 706. All rights reserved 2007.

# Contacts

## The Group of 100

The Group of 100 is an organisation of Chief Financial Officers from Australia's largest business enterprises with a purpose of advancing Australia's financial competitiveness.

### Secretariat

Tel: +61 (0) 3 9606 9661  
e-mail: [g100@group100.com.au](mailto:g100@group100.com.au)  
[www.group100.com.au](http://www.group100.com.au)

## Deloitte

In Australia, Deloitte has 12 offices and over 4,500 people and provides audit, tax, consulting, and financial advisory services to public and private clients across the country. Known as an employer of choice for innovative human resources programs, we are committed to helping our clients and our people excel. Deloitte's professionals are dedicated to strengthening corporate responsibility, building public trust, and making a positive impact in their communities.

For more information, please visit Deloitte's web site at [www.deloitte.com.au](http://www.deloitte.com.au).

### Craig Mitchell

Partner  
Tel: +61 (0) 2 9322 7729  
e-mail: [cmitchell@deloitte.com.au](mailto:cmitchell@deloitte.com.au)  
[www.deloitte.com.au](http://www.deloitte.com.au)

This document is provided as general information only and does not consider your specific objectives, situation or needs. You should not rely on the information in this document or disclose it or refer to it in any document. We accept no duty of care or liability to you or anyone else regarding this document and we are not responsible to you or anyone else for any loss suffered in connection with the use of this document or any of its content.

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, and its network of member firms, each of which is a legally separate and independent entity. Please see [www.deloitte.com/au/about](http://www.deloitte.com/au/about) for a detailed description of the legal structure of Deloitte Touche Tohmatsu and its member firms.

Liability limited by a scheme approved under Professional Standards Legislation.

© 2008 Group of 100 Incorporated. Produced in association with Deloitte Touche Tohmatsu. August 2008. All rights reserved.



## Contact us

Deloitte  
Tel: +61 (0) 2 9322 7000  
[www.deloitte.com.au](http://www.deloitte.com.au)



Tel: +61 (0) 3 9606 9661  
[www.group100.com.au](http://www.group100.com.au)