

group

1000

An association of Australia's senior Finance Executives
from the nation's business enterprises

Guide to Compliance
with ASX Principle 7:
“Recognise and Manage Risk”



Guide to Compliance with ASX Principle 7: “Recognise and Manage Risk”

November 2003

© 2003 Group of 100 Incorporated
ISBN 0-9750205-1-X

Produced in association with

Deloitte.

ASX Principle 7: “Recognise and Manage Risk”

Establish a sound system of risk oversight and management and internal control.

This system should be designed to:

- identify, assess, monitor and manage risk; and
- inform investors of material changes to the company's risk profile.

To achieve best practice:

- Recommendation 7.1 requires the board or appropriate board committee to establish policies on risk oversight and management; and
- Recommendation 7.2 requires the chief executive officer (CEO), or equivalent, and the chief financial officer (CFO), or equivalent, to *state to the board* in writing that:
 - the statement given in accordance with best practice recommendation 4.1 (the integrity of financial statements) is founded on a sound system of risk management and internal compliance and control which implements the policies adopted by the board; and
 - the company's risk management and internal control and compliance system is operating efficiently and effectively in all material respects.
- Recommendation 7.3 requires:
 - the explanation of any departures to Principle 7 to be made in the annual report; and
 - to make publicly available, ideally by posting on the company's website in a clearly marked corporate governance section, a description of the company's risk management policy and internal compliance and control system.

Guide to Compliance with ASX Principle 7: “Recognise and Manage Risk”

Table of contents

Preface	1
Executive Summary	2
1. Introduction	5
2. Principle 7: “Recognise and Manage Risk”	6
3. Detailed Guidance	8
Appendix 1	
Assessing the effectiveness of the company’s risk management and internal control	19
Appendix 2	
Principle 4 and Principle 7: Illustrative wording for CEO and CFO certifications	20
Appendix 3	
Internal control compliance statement: Illustrative wording for Directors’ Report as part of the Annual Report	21
Appendix 4	
Key Sources of Information	22

Preface

Good corporate governance practices are essential to efficient capital markets and investor confidence. Recent developments, both internationally and in Australia, have focussed on these goals. The introduction of the ASX Corporate Governance Council's "Principles of Good Corporate Governance and Best Practice Recommendations", 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 best practice guidelines where appropriate.

This Guide to Compliance with ASX Corporate Governance Council Principle 7: "Recognise and Manage Risk" has been prepared for the Group of 100 by Deloitte. The need for guidance was identified in a series of workshops the Group of 100 held in association with Deloitte to discuss the implications of the ASX 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.

I 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 endorsed the Guide for use by listed entities.

On behalf of the Group of 100 I wish to acknowledge the significant effort and input from Deloitte, the contributions of those Chief Financial Officers who attended the workshops and provided feedback during its development and the National Executive and staff of the Group of 100.

John V. Stanhope
National President
Group of 100

Executive Summary

The ASX Corporate Governance Council's "Principles of Good Corporate Governance and Best Practice Recommendations" 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 Principle 7: "Recognise and Manage Risk".

Formal Framework

Issue: Should the internal control model of the Committee of Sponsoring Organisations of the Treadway Commission (COSO model), 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 model to facilitate compliance with Principle 7. The COSO model is a broadly accepted example on which to base a company's own model and is used as the basis of the guidance in this document.

Breadth of Controls

Issue: How should a company balance its focus on financial risks and controls in respect of the CEO/CFO certification and business risks in respect of the Board's oversight of risk management policies, in accordance with Principle 7?

Guidance: The Board's oversight of risk management policies should encompass operational, financial reporting and compliance risks. The CEO/CFO certification should focus on financial reporting risks and controls and such other risks and controls specified by the Board.

Layers of Controls

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

Guidance: All layers of the COSO 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

Issue: What is an appropriate level of testing and what testing processes should be used in support of the annual control certification by the CEO and CFO and the annual compliance statement in the annual report?

Guidance: A reasonable level of assurance should be obtained from testing. Testing processes adopted are a matter of professional judgment and will vary from company to company but should draw reference from the monitoring layer of COSO.

Period of Coverage

Issue: Does the period of coverage of the internal control certifications required under Principle 7 include the entire reporting period up to and including the date of signing the annual report?

Guidance: The internal control certifications should cover the entire 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 financial report.

Corporate Reach

Issue: If an ASX-listed entity includes a variety of business forms such as subsidiaries, associates and joint ventures, which of these components of the entity 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 in the compliance statement to the annual report.

Operating Efficiently and Effectively

Issue: In making certification under Recommendation 7.2, what is meant by "operating efficiently and effectively"?

Guidance: Consistent with subsequent ASX Corporate Governance Council guidance, "operating efficiently and effectively" should focus on design and operating effectiveness and does not require a specific cost-benefit assessment.

Reporting Templates

Issue: In each of the three areas of disclosure required under Principle 7 (CEO/CFO certification, compliance statement in the annual report, and website descriptions of the control framework), what disclosures are appropriate?

Guidance: Refer Appendices 2 and 3 and the detailed guidance.

1. Introduction

1.1 Background

In March 2003, the ASX Corporate Governance Council released its “Principles of Good Corporate Governance and Best Practice Recommendations” (the Principles), implementing a disclosure-based “if not, why not?” regime for corporate governance. One of these Principles is Principle 7 “Recognise and Manage Risk”.

The Listing Rules of the Australian Stock Exchange (ASX) require listed entities to include a statement disclosing the extent to which they have followed the best practice recommendations of the ASX Corporate Governance Council 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).

Companies are required to disclose compliance with the Principles from financial years commencing on or after 1 January 2003.

The Group of 100, in conjunction with Deloitte, facilitated a series of workshops for its members to discuss the ramifications of these Principles. Following these workshops the Group of 100 National Executive decided that further detailed guidance in respect of Principle 7 would be useful to members and facilitate compliance.

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 Principle 7. Implementation of the guidance may require judgment to be exercised in ensuring compliance with the recommendations.

The Group of 100 believes that compliance with this Guide will facilitate in establishing 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) two other similar internal control frameworks - the Combined Code in the United Kingdom and the Sarbanes-Oxley regime in the United States.

It is envisaged that this guidance may be revised from time to time.

2. Principle 7: “Recognise and Manage Risk”

2.1 What is Principle 7: “Recognise and Manage Risk”?

Principle 7 requires companies to establish a sound system of risk oversight and management and internal control.

This system should be designed to:

- identify, assess, monitor and manage risk; and
- inform investors of material changes to the company's risk profile.

To achieve best practice:

- Recommendation 7.1 requires the board or appropriate board committee to establish policies on risk oversight and management; and
- Recommendation 7.2 requires the chief executive officer (CEO), or equivalent, and the chief financial officer (CFO), or equivalent, to *state to the board* in writing that:
 - the statement given in accordance with best practice recommendation 4.1 (the integrity of financial statements) is founded on a sound system of risk management and internal compliance and control which implements the policies adopted by the board; and
 - the company's risk management and internal control and compliance system is operating efficiently and effectively in all material respects.
- Recommendation 7.3 requires:
 - the explanation of any departures to Principle 7 to be made in the annual report; and
 - to make publicly available, ideally by posting on the company's website in a clearly marked corporate governance section, a description of the company's risk management policy and internal compliance and control system.

2.2 Key Issues Surrounding Principle 7: “Recognise and Manage Risk”

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

- **Formal Framework:** Should the internal control model of the Committee of Sponsoring Organisations of the Treadway Commission (COSO model), on which both the UK and US regulatory frameworks are built, also be adopted by Australian companies?
- **Breadth of Controls:** How should a company balance its focus on financial risks and controls in respect of the CEO/CFO certification and business risks in respect of the Board’s oversight of risk management policies, in accordance with Principle 7?
- **Layers of Controls:** If the COSO model is adopted, should companies implement controls at all layers of the COSO model and, if so, with what relative importance? How can these controls be most effectively implemented and maintained?
- **Level of Assurance:** What is an appropriate level of testing and what testing processes should be used in support of the annual control certification by the CEO and CFO and the annual compliance statement in the annual report?
- **Period of Coverage:** Does the period of coverage of the internal control certifications required under Principle 7 include the entire reporting period up to and including the date of signing the annual report?
- **Corporate Reach:** If an ASX-listed entity includes a variety of business forms such as subsidiaries, associates and joint ventures, which of these components of the entity should be included in the scope of Principle 7 compliance activities?
- **Operating Efficiently and Effectively:** In making certification under Recommendation 7.2, what is meant by “operating efficiently and effectively”?
- **Reporting Templates:** In each of the three areas of disclosure required under Principle 7 (CEO/CFO certification, compliance statement in the annual report, and website descriptions of the control framework), what disclosures are appropriate?

3. Detailed Guidance

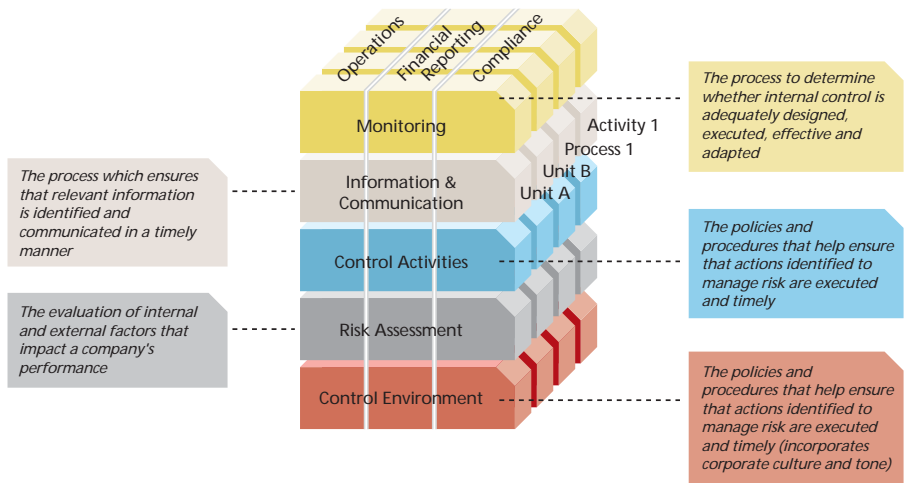
3.1 Formal Framework

Issue: Should the internal control model of the Committee of Sponsoring Organisations of the Treadway Commission (COSO model), on which both the UK and US regulatory frameworks are built, also be adopted by Australian companies?

The ASX Corporate Governance Council Principles do not specify or recommend the use of any specific risk management and internal control framework. Consequently, the COSO model has been suggested to be an effective framework.

In 1992, the Committee of Sponsoring Organisations of the Treadway Commission (COSO) developed a formal framework for implementing and maintaining a system of risk management and internal control, known as the COSO model. (The Group of 100 notes that this model is currently being enhanced.) A diagrammatic representation of the 1992 COSO model is shown in Diagram 1, and further information is available at www.coso.org.

Diagram 1 - Layers of Control



The COSO model is recognised explicitly in the Sarbanes-Oxley internal control regime and implicitly in the UK Combined Code internal control regime.

The Group of 100 recognises that the COSO model is considered the preferred global framework for risk management and internal control. However, the Group of 100 also recognises that because of the diversity of companies, due to such factors as their size, complexity and culture, companies should have flexibility in developing their own risk management and internal control model and, in doing so, should have regard to the recognised COSO model.

Guidance: Each company should have its own documented risk management and internal control model to facilitate compliance with Principle 7. The COSO model is a broadly accepted example on which to base a company's own model and is used as the basis of the guidance in this document.

3.2 Breadth of Controls

Issue: How should a company balance its focus on financial risks and controls in respect of the CEO/CFO certification and business risks in respect of the Board's oversight of risk management policies, in accordance with Principle 7?

The current 1992 COSO model identifies three categories of risks and controls, namely:

- operations;
- financial reporting; and
- compliance.

Recommendation 7.1 of the Principles and its commentary and guidance suggests that a broad approach to risk oversight and management should be adopted. Such an approach would suggest that all three COSO categories of risks and controls be covered.

The Board's risk and control compliance statement in the annual report should disclose this broad approach and disclose that the CEO/CFO certification Recommendation 7.2 has been received and considered (Appendix 3).

Recommendation 7.2 of the Principles makes reference to Recommendation 4.1 in regard to the integrity of the financial statements. This suggests that the annual control certification by the CEO and CFO to the Board should focus primarily on risks and controls relating to the integrity of the company's financial reporting.

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

The Group of 100 considers that Recommendation 7.2 is designed to supplement the broad nature of Recommendation 7.1 by requiring the CEO's and CFO's certification in respect of the financial reporting process.

The Group of 100 acknowledges that the Board may seek additional assurance or certification pertaining to other areas of risk oversight and management. This will require the CEO and CFO certifications to clearly state that they relate to controls over the integrity of financial reporting and such other risks and controls specified by the Board (refer Appendix 2).

Guidance: The Board's oversight of risk management policies should encompass operational, financial reporting and compliance risks. The CEO/CFO certification should focus on financial reporting risks and controls and such other risks and controls specified by the Board.

3.3 Layers of Control

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

As shown in Diagram 1 above, there are 5 “layers” of control in COSO, each providing a different element of the overall control framework. Both Sarbanes-Oxley and the Combined Code reference the need for all five COSO layers to be addressed in a company’s system of internal control. While different degrees of emphasis exist between COSO layers in these overseas frameworks, there is no express distinction of importance between layers.

The Group of 100 notes that for the COSO model to operate effectively all layers need to co-exist and operate collectively while recognising that each “higher” layer is dependent upon its underlying layers.

The process of effectively implementing and maintaining controls for each of the COSO layers will vary from company to company. In designing an effective 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; and
- cost-benefit issues.

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

The following non-exhaustive listing has been drawn from the ‘Commentary and guidance’ to Principle 7 and other corporate best practice to provide examples of how, depending on a company’s circumstances, controls can be effectively implemented and maintained over the five COSO layers:

COSO Layer	Layer Examples
Control Environment	Code of Conduct Corporate Culture/Values/Tone/Commitment External regulatory environments
Risk Assessment	Utilise AS/NZS 4360 - Risk Management ¹ Risk registers Risk-control matrices (and linked to internal audit program)
Control Activities	Policies and procedures manuals Process flowcharts Inventory of controls (including accountabilities)
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 (eg., risk management committees) Internal audit function Control self assessments

1 Currently undergoing revision.

The Group of 100 encourages appropriate and regular corporate profiling and/or training to reinforce and refresh controls in place for each COSO layer.

Guidance: All layers of the COSO 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.

3.4 Level of Assurance

Issue: What is an appropriate level of testing and what testing processes should be used in support of the annual control certification by the CEO and CFO and the annual compliance statement in the annual report?

Principle 7 explicitly requires an annual certification by the CEO and CFO to the Board in relation to the operating effectiveness and efficiency of controls. The ASX Listing Rules require a statement in the annual report disclosing the extent of compliance with the ASX Corporate Governance Council Principles. In order to provide this assurance a level of testing must be undertaken.

No guidance is available in respect of the assurance and testing processes required in support of ASX Corporate Governance Council Principle 7 certifications and statements.

For the equivalent certification requirements under the Sarbanes-Oxley regime, prescriptive guidance is available in relation to the nature, extent and documentation of tests required to provide the relevant high level of assurance (refer the American Institute of Certified Public Accountants website listed in Appendix 4).

In accordance with guidance in the Combined Code, the Board must undertake due and careful enquiry having regard to the nature of the company. The Combined Code also prescribes the need to conduct an annual control assessment and periodically review the need for an internal audit function.

The Group of 100 considers that the level of testing adopted is a matter of professional judgment and will vary from company to company. This should ensure consistency with the UK regime while avoiding the prescriptive nature of the Sarbanes-Oxley regime.

Due to its nature, any internal control assurance activity is not designed to detect all weaknesses in control procedures because it is not performed throughout the period, audit evidence is often persuasive rather than conclusive and the tests performed are on a sample basis.

The Group of 100 believes that a sufficient amount of testing should be performed to ensure that the financial report is materially correct. This would imply a reasonable level of assurance having regard to the directors' declaration required to be made in the financial report and the external audit opinion attached thereto.

This control assurance will generally be obtained from applying the monitoring layer of the COSO model and may include the following:

- a regular program of internal audits (linked to the risk-control matrix);
- periodic and comprehensive control self-assessments, with independent follow-up; and
- specific and specialised assurance activities in high risk areas appropriate to the company (this may cover areas such as information security and treasury).

All testing and conclusions reached should be fully documented. Reference should be made to Australian Auditing Standard 810 "Special Purpose Reports on the Effectiveness of Control Procedures", where appropriate. Further guidance is include in Appendix 1.

Guidance: A reasonable level of assurance should be obtained from testing. Testing processes adopted are a matter of professional judgment and will vary from company to company but should draw reference from the monitoring layer of COSO.

3.5 Period of Coverage

Issue: Does the period of coverage of the internal control certifications required under Principle 7 include the entire reporting period up to and including the date of signing the annual report?

It is explicit in the ASX Listing Rules that the company's statement of compliance in relation to the ASX Corporate Governance Council Principles in the annual report must cover the entire reporting period, and it is therefore implicit that the certification of financial controls by the CEO and CFO in Recommendation 7.2 should also cover the entire reporting period. (This is different to the Sarbanes-Oxley regime which requires certification at a point in time.)

The ASX Listing Rules also require that the compliance statement in the annual report be current as at a date within six weeks of when the annual report is sent to shareholders, which in nearly all cases is more than six weeks after balance sheet date.

This, therefore, implies that in addition to the certification of controls for the reporting period (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 timing practicalities of this certification, the Group of 100 considers that, in addition to the statements made for the reporting period and 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).

The ASX Corporate Governance Council Principles are not required to be adopted until the first financial year commencing on or after 1 January 2003. Early adoption of the Principles is encouraged by the ASX.

Guidance: The internal control certifications should cover the entire 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 financial report.

3.6 Corporate Reach

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

No guidance is currently provided in the ASX Corporate Governance Council Principles as to whether or not subsidiaries, associates or joint ventures are included in the disclosures required under Principle 7.

Other similar regimes differ slightly in their treatment of this issue. Under Sarbanes-Oxley, only consolidated subsidiaries and the parent company are required to be included in the scope of coverage. For the Combined Code, subsidiaries are included within the scope and whether material joint ventures and associates are included is optional. 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 for the Australian environment. Guidance on the application of materiality is included in AASB 1031 'Materiality'. (Refer Appendix 3 for disclosure.)

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 in the compliance statement to the annual report.

3.7 Operating Efficiently and Effectively

Issue: In making certification under Recommendation 7.2, what is meant by “operating efficiently and effectively”?

Recommendation 7.2 of the ASX Corporate Governance Council Principles, indicates that the CEO and CFO certification on internal controls must refer to a company’s systems as having operated “efficiently and effectively” throughout the reporting period. Certification in respect of the efficiency of controls is not an element of either Sarbanes-Oxley or Combined Code regimes, although the Combined Code does suggest that the cost effectiveness of controls in relation to their corresponding risks be considered when implementing controls.

Subsequent ASX Corporate Governance Council guidance (*refer Guidance to Implementation of Principle 7 at www.asx.com.au*) clarifies that the word “efficiently” should not be read in isolation but together with the word “effectively” to focus on two elements:

- design effectiveness - whether the system is appropriately designed to enable effective risk management; and
- operating effectiveness - whether the system is operating effectively to achieve the desired business outcomes.

The ASX Corporate Governance Council notes that the achievement of business outcomes is key to measuring operating effectiveness. It also notes that outside events may lead to undesirable business outcomes which does not necessarily mean that the systems in place are ineffective. The Group of 100 concurs with this view.

The assessment of the effectiveness of system controls in achieving a company’s business outcomes should be fully documented and, if appropriate, be referenced to the company’s strategic plan.

Guidance: Consistent with subsequent ASX Corporate Governance Council guidance, “operating efficiently and effectively” should focus on design and operating effectiveness and does not require a specific cost-benefit assessment.

3.8 Reporting Templates

Issue: In each of the three areas of disclosure required under Principle 7 (CEO/CFO certification, compliance statement in the annual report, and website descriptions of the control framework), what disclosures are appropriate?

The ASX Corporate Governance Council did not prescribe the content, format or style of the annual report and CEO/CFO certifications required under the ASX Corporate Governance Council Principles – consistent with the philosophy of open disclosure and an “if not, why not?” regime.

Notwithstanding this, there is a clear desire by companies to drive efficiencies in their compliance processes through adopting accepted or common standards wherever possible. The Group of 100 recognises that opportunities exist for Australian companies to leverage the existing reporting standards and norms established by the Sarbanes-Oxley and Combined Code regimes.

The CEO and CFO not only have an internal control certification requirement under Principle 7 but also are required to certify the financial report in accordance with Principle 4 “Safeguarding Integrity in Financial Reporting”. Appendix 2 illustrates an example of a joint certification.

In respect of the internal control compliance statement in the annual report regarding compliance with the ASX Corporate Governance Council Principles (which relates to all principles, not just Principle 7), the Group of 100 is of the view that companies should keep this certification concise and focussed, with appropriate references to the supporting description of the company’s internal control framework and other corporate governance practices. Appendix 3 illustrates a sample certification statement for inclusion in the directors’ report .

As set out in the commentary to Principle 7, material to be disclosed in the corporate governance section of a company’s website should include a description of the company’s risk management policy and internal compliance and control system. This website disclosure will vary from company to company with some parts also relevant for the annual report. The Group of 100 suggests that descriptions of the control framework published on this section of a company’s website would normally include:

- details of the company’s risk management and internal control model (or a reference to the COSO model if adopted by the company);
- information on the key risk exposures of the company;
- concise and focussed descriptions of the key internal control processes adopted and relied upon by the directors for minimising the impact of the key risk exposures and ensuring compliance with the Principles (for example, internal audit function, control self-assessment, etc); and
- the procedures directors have performed in reviewing the effectiveness of the internal control processes in the previous 12 months.

Guidance: Refer Appendices 2 and 3 and the detailed guidance above.

Appendix 1

Assessing the effectiveness of the company's risk management and internal control

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

In order to assist the CEO and CFO in discharging their responsibility to report on internal controls the following template may be useful for documentary purposes. A non- exhaustive list of issues to consider to identify specific controls has been included. The template and issues to consider should be adapted to the company's particular circumstances, such as for multiple locations.

COSO Criteria	Specific Controls Identified (example issues to raise to identify controls)	How controls evaluated?	Assessment of Controls 1-5 (Weak-Strong)
Control Environment and Control Activities	<ol style="list-style-type: none"> 1. Are the directors and management committed to leadership by example? 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? 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? 5. Do employees have the knowledge, skills and tools to support the achievement of the company's objectives and to effectively manage its risks? 6. Are controls adjusted as new risks or operational deficiencies are identified? 7. Is there a professional approach to financial reporting in compliance with Australian Accounting Standards? 	(eg internal audit - date)	
Risk Assessment	<ol style="list-style-type: none"> 1. Are the company's objectives clear? 2. Are significant operations, financial and compliance risks assessed on an ongoing basis? 3. Are the risks which are acceptable to the board clearly understood by management and employees? 		
Information and communication	<ol style="list-style-type: none"> 1. Is 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 its intervention? 2. Do business continuity/disaster recovery plans exist for IT monitoring and reporting systems? 3. Is there an established system of communication for individuals to report suspected breaches of laws or regulations? 		
Monitoring Controls	<ol style="list-style-type: none"> 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? 2. Are changes in the business or its environment which may require changes to the system of internal control identified? And are there procedures to ensure that appropriate corrective action is taken in response to the risk and control assessments? 3. Is there communication to the board on the effectiveness of ongoing monitoring? 		

Appendix 2

Principle 4 and Principle 7 :

Illustrative wording for CEO and CFO certifications

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 statements and notes thereto comply with Accounting Standards in all material respects;
 - (ii) 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;
 - (iii) in our opinion, the financial statements and notes thereto are in accordance with the Corporations Act 2001; and
 - (iv) 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 compliance and 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 compliance and control systems which, in all material respects, implement the policies adopted by the board of directors;
 - (ii) the risk management and internal compliance and control systems to the extent they relate to financial reporting [specify other, if any] are operating effectively and efficiently, in all material respects, based on the [risk management model adopted by the company]; and
 - (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

[Date of annual report]

Chief Financial Officer

[Date of annual report]

Appendix 3 ---

Internal control compliance statement:

Illustrative wording for Directors' Report as part of the Annual Report

Risk and Control Compliance Statement

Under ASX Listing Rules and the ASX Corporate Governance Council's "Principles of Good Corporate Governance and Best Practice Recommendations" (the Principles), the company is required to disclose in its annual report the extent of its compliance with the Principles.

The directors have implemented internal control processes for identifying, evaluating, and managing significant risks to the achievement of the company's objectives. These internal control processes cover financial, operational and compliance risks. The company's corporate governance practices are outlined in further detail below.

[Insert details or reference separate section]

The directors have received and considered the annual control certification from the Chief Executive Officer and the Chief Financial Officer in accordance with the Principles relating to financial [specify other, if any] risks.

Material associates and joint ventures, which the company does not control, are not dealt with for the purposes of this statement.

Throughout the reporting period, and as at the date of signing of this annual report, the company was in compliance with the Principles in all material respects.

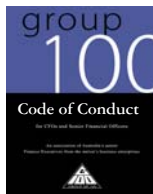
** Interchange company with group or consolidated entity as appropriate.*

Appendix 4

Key Sources of Information

1. ASX Corporate Governance Council:
www.asx.com.au/about/CorporateGovernance_AA2.shtm
2. CLERP Paper No 9:
www.treasury.gov.au/contentitem.asp?pageld=&ContentID=700
3. COSO Model:
www.coso.org
4. Sarbanes-Oxley Act of 2002 (US):
www.sec.gov/about/laws.shtml
5. American Institute of Certified Public Accounts (AICPA):
www.aicpa.org/sarbanes/index.asp
6. The Combined Code (UK):
www.frc.org.uk/combined.cfm
7. Institute of Chartered Accountants in England and Wales Guidance:
www.icaew.co.uk/internalcontrol
8. Standards Australia (AS/NZS 4360 Risk Management):
www.standards.com.au
9. Group of 100 Inc:
www.group100.com.au
10. Deloitte
(click on Services then Corporate Governance Reform):
www.deloitte.com.au

Other Group of 100 publications available on our website



www.group100.com.au



Group of 100 Incorporated
385 Bourke Street (Level 28)
Melbourne
Tel: (03) 9606 9661
E-mail: g100@group100.com.au
Web site: www.group100.com.au