



Principle 7:  
Recognise and Manage Risk  
Guide for small – mid  
market capitalised companies



# Quick start guide

Use the quick start guide below to help you navigate through the guide

Action	Reference in the guide	Has action been completed?
Complete risk tolerance questionnaire	4.1	<input type="checkbox"/>
Draft Risk Management Policy	4.2	<input type="checkbox"/>
Approve Risk Management Policy	4.2	<input type="checkbox"/>
Publish Risk Management Policy on the company website	4.2	<input type="checkbox"/>
Review board charter and role descriptions to ensure accountability for risk is included	4.3	<input type="checkbox"/>
Identify material business risks and document in the risk register in year and continue to reassess the full list of risks in consecutive years	5.1	<input type="checkbox"/>
Allocate risk owners to critical risks	5.1	<input type="checkbox"/>
Manage material business risks	5.2	<input type="checkbox"/>
Update the risk register or prepare individual risk reports and present to the board	5.3	<input type="checkbox"/>
Prepare CEO/CFO certification	5.3	<input type="checkbox"/>
Prepare a summary of the risk management activity throughout the year and present to the board (including effectiveness statement)	5.3	<input type="checkbox"/>
Prepare annual report disclosure with respect to Recommendation 7.4 under Principle 7	6	<input type="checkbox"/>

# Foreword

ASX Markets Supervision (ASXMS) is delighted to present this Guide to Reporting on Risk for the purposes of ASX Listing Rule 4.10.3 and, hence, Principle 7 of the ASX Corporate Governance Council *Corporate Governance Principles and Recommendations* (Principles).

Risk management is an element of corporate governance which is under increased focus – a focus which is rising and has been elevated further since the global financial crisis. The Principles identify risk management practices which listed entities must report against in their annual reports on an ‘if not, why not’ basis. Accordingly, while the Principles do not mandate these practices, it is for listed entities to disclose and explain the extent to which they have not followed the recommendations set out in the Principles, and give reasons for not following them if that is the case.

ASXMS has identified that small to mid-capitalised ASX-listed entities may experience difficulty in implementing risk management practices which accord with the recommendations in the Principles due to the generally lower level of resources available to such entities. The purpose of this Guide is to allow small to mid-capitalised ASX-listed entities to access information and guidance on the management of material business risks in a way that will allow them to report positively against the recommendations in Principle 7.

The ASX Listing Rules require a listed entity to report in its annual report on the extent to which it has followed the Principles during the reporting period. Many listed entities may find themselves in a position of having commenced a review of how they manage risk and whether it accords with the recommendations in the Principles towards the end of a particular reporting period. ASXMS encourages such entities to identify that they have commenced this process so that their stakeholders will be aware that this is the case.

ASXMS would like to thank our partners in the production of this Guide – Deloitte and Blakiston & Crabb. Together they have assisted ASXMS in identifying the need and delivering a solution. The production of this Guide in June 2009 will be accompanied by a series of national seminars to introduce the Guide and explain how best to use it. These will be followed, where the demand exists, by workshops to answer more detailed questions from entities which have commenced the process of managing their material business risks in accordance with the recommendations in Principle 7 and with the assistance of this Guide.

This program is made possible by the ASX Markets Supervision Education and Research Program. The Program uses the proceeds of fines and settlements from ASX’s Disciplinary Tribunals (less certain expenses in taking matters before the Tribunals), to raise awareness of and promote compliance with ASX’s supervisory requirements and supervisory issues in ASX’s markets and promote the integrity of ASX’s markets and/or promote confidence in their integrity.



Eric Mayne  
Chief Supervision Officer  
ASX Markets Supervision  
June 2009



# 1. Introduction

Risk management is a journey. It is not achieved overnight nor is there a 'standard answer'. It will take your company time to establish and needs to be regularly re-tuned to your company's changing circumstances. Each company will ultimately establish its own unique level of risk maturity appropriate for its environment, industry and stakeholder expectations.

When the ASX Corporate Governance Council released the second edition of the *Corporate Governance Principles and Recommendations* (Principles), they made significant changes to *Principle 7: Recognise and Manage Risk* (Principle 7). The new Principle 7 reflects the increasing expectations of stakeholders (including supervisors and regulators) as to how listed companies should manage risk.

## Foundations of Principle 7

The purpose of Principle 7 is to ensure appropriate disclosure and communication to stakeholders on matters of risk and that the collective corporate mind of the company is focused on effectively managing material business risks. A key part of satisfying the requirements of Principle 7 is documentation – once this documentation is established then the ongoing effort is reduced. However, companies should not fall into the trap of simply rolling forward the prior year's documentation. It is the risk management process itself and re-consideration of risks and their management that is key to ensuring ongoing reporting against the recommendations of Principle 7.

Successful reporting against the recommendations of Principle 7 also depends on having the right company culture, the right attitude to risk management and ensuring the right decisions and actions are made in times of pressure.

*Tip: Regularly discussing culture and attitude to risk amongst senior management and the board and communicating these expectations with other staff is an important foundation of risk management.*

## Use of guide

This guide is designed to assist those companies that are at the very beginning of their risk journey. It aims to be a practical tool to help small to medium capitalised companies to understand the expectations of supervisors, regulators and the wider market about how they manage risk and consequently how they can begin to meet their reporting obligations in relation to Principle 7. The guide sets out a process with supporting educative materials and pro-forma templates that, if followed by the board and management, should assist small and medium listed companies to establish for themselves a sound system of risk management by populating templates according to their own circumstances. This will enable companies to avoid a 'tick a box' approach, where suggested or recommended outcomes are simply copied without due thought or process.

A checklist has been included in Appendix I at the end of the guide to assist the reader.

## 2. What are material business risks?

Risks relate to future events or situations that provide opportunities or create an exposure for the company.

Risks are not absolute but represent a degree of probability or chance that they may or may not occur. While all risks need to be understood and managed, Principle 7 focuses specifically on risks that may have a material impact on the company (material business risks). In other words, risks that could have an adverse impact on shareholder value and the legitimate interests of other stakeholders.

Material business risks should not be seen purely from a financial perspective. Examples of material business risk categories identified in Principle 7 that could have significant reputational, as well as financial impact, include:

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

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 a genuine connection with the business
- material business risks should be considered at a whole-of-company level.



Risk management is not about eliminating all risks, it is about identifying and responding to risks in a way that creates value for a company and its shareholders



# 3. Why manage material business risks?

---

All companies will face some risks which have the potential to significantly or materially impact their performance. Risks are inherent in every action companies take.

Why do risks need to be managed? Put simply, managing risks is the right thing to do. Commercial drivers for risk management include:

- the effect of the global financial crisis has exposed companies to risks they have never experienced before
- institutional investors are asking more pointed questions about risk
- providers of director and officer liability insurance (D&O) have a vested interest in ensuring that the board is mitigating and disclosing material business risks
- satisfying the reporting requirements of Principle 7.

However, risk management is not about eliminating all risks, it is about identifying and responding to risks in a way that creates value for a company and its shareholders. For any company that hopes to compete and grow, a long-term strategy needs to involve risk-taking for reward.

Ignoring material business risks on the basis of cost restrictions is not justifiable. All listed companies can, and are expected to, gear themselves for appropriately managing risk and make positive disclosures of what they are doing under the 'if not, why not' regime.

*Tip: Clearly know your company-wide strategy/plan – this is the starting point to understanding your corporate risks.*

# 4. Pre-requisites for managing material business risks

A sound framework of risk oversight, risk management and internal control is fundamental to good corporate governance. It underpins reliable financial reporting, compliance with relevant laws and regulations, and effective and efficient operations. Before material business risks can be managed, thought needs to be given to:

**Action:**  
Complete risk tolerance questionnaire (Appendix A)

## 4.1 Understanding your company's overall risk tolerance

Risk tolerance is the amount of total risk that a company is prepared to accept or be exposed to at any point in time. It can be viewed in one sense as the organisation's attitude towards risk management.

Given its responsibility for representing the interests of shareholders, the company's board plays a vital role in overseeing management's approach to risk management, including the determination of the company's tolerance for risk. The risk tolerance should be set by the board in conjunction with the chief executive officer (CEO) and clearly communicated to management. When a company considers tolerance for risk this does not mean that management will seek risk per se; it means the company will accept risk if suitably rewarded.

The risk tolerance should drive the overall risk management effort and determine the action required to address material business risks. As willingness to accept risk decreases, the complexity and maturity of risk management effort increases as depicted by the diagram below.

To further illustrate this direct correlation, compare the tolerance for taking risk between a small exploration company and a major blue chip 'pillar of society' company. The stakeholder profiles are vastly different – consequently the tolerances for risk would be different as well to reflect its stakeholder expectations. The small exploration company would generally accept a higher level of risk with a lower level of risk management effort to reflect its stakeholder expectations. Vice versa, the major blue chip company would generally have a much higher level of risk management effort reflective of the lower willingness of the company and stakeholders to accept risk.

The short questionnaire in Appendix A will help you understand some of the factors which can impact on your company's attitude towards risk.

**Tip:** The board and senior management should have a clear understanding of what the company's risk tolerance is and the extent to which they wish to manage risk. This should be reconsidered at least annually.



**Action:**

*Publish risk management policy on the website*

**4.2 Risk management and oversight policy**

A company's risk management policy should be designed to document the company's risk management approach, its willingness to accept risk, accountabilities for managing risk, and the resources and processes dedicated to the management of risk. It should ideally include and be reflective of a set of objectives that guide and shape risk management activities, and outline how performance against these objectives will be measured.

The strength of risk management processes adopted and summarised in the risk management policy will also depend on the company's overall risk tolerance as determined in section 4.1 above.

Appendix B provides an outline of what should be included in a risk management policy. This policy and descriptions should not be 'boilerplate'. It should reflect the actual activities undertaken by the company and its attitude and approach to managing material business risks.

*Tip: Senior management is responsible for establishing, documenting and maintaining the risk management policies. Independent board members should oversee these documented risk management policies to ensure they are sufficiently clear and in line with the company's overall risk tolerance and expectations of stakeholders.*

**Recommendation 7.1 under Principle 7**

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



**Action:**

*Review Board Charter and role descriptions to ensure accountability for risk is included.*

**4.3 Accountability and responsibility**

While managing material business risks should be the responsibility of everyone in the company, specific accountability should be reflected in a company’s structure and organisational chart and these accountabilities should be clearly defined in the role, charter and responsibilities of the company’s board and management team.

For specific material business risks, accountability should also be assigned to appropriate individuals who will report on the status and management of these risks to the board. Companies can use a risk register to document this requirement. An example of useful information to be captured in a risk register is provided in Appendix C.

An individual should be charged with implementing the risk management process and establishing a process to ensure that the reporting requirements of the Principle 7 are met. In small – mid cap companies this is often the company secretary or the CFO. An example of other accountabilities within a small – mid cap company is provided below:

Overall responsibility for risk management process	Company secretary or CFO
Overall responsibility for all material business risks	Chief Executive Officer
Responsibility for individual material business risks (in conjunction with CEO):	
• financial risks	CFO (or equivalent)
• operations	COO (or equivalent)
• technology	CIO (or equivalent)
• human resources	Head HR (or equivalent)
• compliance	Company secretary
• etc.	

Appendix D lists more example accountabilities and responsibilities for managing risk in a company.

*Tip: Consider including appropriate risk Key Performance Indicators into the management performance agreements.*

**4.4 Integration/timing**

There are increased expectations that the board and management are effectively managing the material business risks. For these reasons, risk management should be embedded in all of the company’s practices and business processes so that it is relevant, effective and efficient.

In particular, risk identification should be embedded into:

- strategic and operational planning
- management and board decision making
- project planning and execution
- change management processes.

Risk management should not be a “bolt on” to the company’s existing processes. It should be something management considers every day as part of their job. By integrating risk management with existing company processes, management can ensure the efficient use of resources and therefore reduce the potential for duplication of effort when working to reduce risk levels. Another key benefit of integration is that it helps ensure that the risk management process itself is appropriately resourced and remains relevant and sustainable.

# 5. How to manage material business risks?

While there is unlikely to be a one-size-fits-all solution to how companies address risk, there are some common approaches.

Appropriate management and documentation of material business risks is essential. This could be as simple or as complicated as suits your business. However, it should include the following common activities:

- identify material business risks
  - identify the risks faced by the business
  - prioritise/rank the risks based on an agreed definition of significance.
- manage material business risks
  - address the risk where necessary
  - identify and ensure the operation of key control measures.
- internally report on material business risks
  - management to communicate appropriately and fairly to the board.

## Recommendation 7.2

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



**Action:**

Complete the first section of the risk register (Appendix C)

**5.1 Identify material business risks**

**Identify the risks faced by the business**

The aim of this process is to develop a risk register with a list of material business risks (risk profile) based on those events that might enhance, prevent, degrade or delay the achievement of the business objectives. It is equally important to identify the risks associated with not pursuing an opportunity.

Material business risks should be identified at the most senior level within the company and be documented in the context of the company’s strategy and objectives. Both the sources of risks and their potential consequences should be identified. Material business risks should be validated with the board to ensure their perspective on business vulnerabilities is taken into account.

*Tip: In identifying material business risk, think above and outside of your day-to-day job. Think company-wide and from your stakeholders’ perspectives (e.g. shareholders, lenders, suppliers, employees, customers, community, etc) as well as external environment.*

Sufficient management time needs to be allocated to risk identification, because a risk that is not identified at this stage will not be included in any further analysis in the yearly cycle. Identification should include risks whether or not their source is under the control of the company (e.g. change in government policy). There is no generally accepted number of material business risks that companies should focus on; the list should not be too small, as risks may be missed and not too large as the management team will have difficulty in focussing on the key issues.

Risk identification can be undertaken as part of the existing strategic planning or budgeting process, or can be carried out as a process of its own through a facilitated workshop with the management team and potentially the board. These workshops can be facilitated by an external provider or by appointing a member of the management team to act as facilitator. This will help to minimise business interruption.

Appendix C contains an example of a risk register that can be populated as part of this process.

*Tip: Reach consensus early on your understanding (or definition) of what each material business risk represents.*





**Action:**  
*Complete the third section of the risk register (Appendix C)*

## 5.2 Manage material business risks

Prioritised material business risks should be compared with the risk tolerance established in the risk management policy.

Where the level of risk is above the desired level (as outlined in Appendix E), management should develop and execute an action plan to address the risk in one of the following ways:

- **transfer the risk** through the use of contracts or insurance arrangements. Risk can be transferred to another party which has greater control over the risk situation, or is less susceptible to the impact of the risk factors. It is important to understand however that responsibility for overseeing the risk cannot be transferred or outsourced as ultimate accountability for the risk rests with the company management
- **reduce the risk** by adopting alternative approaches to achieving the same objective. For example, in the case of a risk to a project, the treatment strategy might involve identifying an alternative course of action such as revised timing, a different delivery model, a different resource mix or increased controls. Each may reduce the risk likelihood or eliminate the risk altogether
- **accept the risk** and develop contingency plans to minimise the impact should the risk eventuate. For the risks accepted to be managed, it is necessary to identify an individual responsible for establishing a monitoring process that captures the likelihood of the risk occurring and the treatment strategies to be applied should the risk eventuate. Consideration should be given to continuous disclosure requirements under the ASX Listing Rules.



When selecting risk treatment options, the company should consider the values and perceptions of stakeholders and the most appropriate ways to communicate with them. Though equally effective, some risk treatments can be more acceptable to some stakeholders than others. Where risk treatment options can impact on risk elsewhere in the company, these areas should be involved in the decision.



### 5.3 Report on material business risks

Ongoing reporting and discussion of the management of material business risks at the board level is a crucial step in the process.

Risk reporting is a key factor for the board in its strategic planning and the management of risk across the company.

Assurance over this risk reporting and the underlying controls associated with material business risk (and financial reporting risks) is not required, however the board may request independent verification for some or all of the risk management processes or individual controls. For small – mid cap companies a peer review by an independent director often provides the required comfort over the risk management process and related controls. Other alternatives include using external providers to provide focussed ‘internal audit-like’ services.

The table below outlines the flow of risk reporting throughout a year where activities are aligned to quarterly board meetings:

	Quarter one	Quarter two	Quarter three	Quarter four (full year)
Management	<ul style="list-style-type: none"> <li>complete risk tolerance questionnaire</li> <li>document Risk Management Policy</li> <li>publish Risk Management Policy on the company website</li> <li>review board charter and role descriptions to ensure accountability for risk is included</li> <li>identify material business risks and present full company risk profile</li> <li>allocate risk owners to critical risks.</li> </ul>	<ul style="list-style-type: none"> <li>present updated risk register or individual risk reports.</li> </ul>	<ul style="list-style-type: none"> <li>present updated risk register or individual risk reports.</li> </ul>	<ul style="list-style-type: none"> <li>update risk register or individual risk reports and present to the board</li> <li>CEO/CFO certification on Recommendation 7.3 of Principle 7</li> <li>summary of annual risk management effort</li> <li>prepare annual report disclosure with respect to Recommendation 7.4 of Principle 7.</li> </ul>
Board	<ul style="list-style-type: none"> <li>agree and set the company’s overall risk tolerance</li> <li>approve Risk Management Policy</li> <li>provide input into the full company risk profile.</li> </ul>	<ul style="list-style-type: none"> <li>note updated risk register or individual risk reports and question management if required.</li> </ul>	<ul style="list-style-type: none"> <li>note updated risk register or individual risk reports and question management if required.</li> </ul>	<ul style="list-style-type: none"> <li>note updated risk register or individual risk reports</li> <li>note CEO and CFO certification</li> <li>note the summary of annual risk management effort (including effectiveness statement).</li> </ul>

**Action:**

Complete the fourth section of the risk register (Appendix C) or individual risk report (Appendix F)

**Risk reporting throughout the year**

Principle 7 requires the board to report whether they have received an assurance from management that management has identified and addressed the material business risks effectively. This assessment should occur at the individual material business risk level and, in order to support the focus on risk throughout the year (and to ease the workload), it is normally suggested that this risk reporting to the board occurs throughout the year.

The most common way to communicate the company's material business risks to the board is for each risk owner to present an updated risk register (Appendix C) that summarises the significance of each risk as well as actions taken by management to mitigate the risks since they were originally identified.

It is important to recognise however, that a company's risk profile and therefore the risk register will evolve over time as risk priorities change through changes in a company's activities, in the external environment and as a result of the progressive implementation of treatment strategies, therefore risk reporting needs to be continuous.

Managers who have ownership over material business risks, at their discretion, may choose to prepare and present to the board a more detailed individual risk report. An individual risk report (as outlined in Appendix F) provides the appropriate discipline in managing and reporting of material business risks. These reports normally include:

- risk description and outline of likely consequences of risk eventuating
- current controls that help to reduce the likelihood or consequence of the risk
- assurance on the effectiveness of current controls
- risk level based on the company's policy or framework
- further management action required to minimise the risk.

Similar to reporting using the risk register, individual risk reports should be discussed at the board level as part of existing board meetings. Linking risk reporting to existing monthly or quarterly board reporting can help improve the timeliness and quality of communication.

*Tip: Consider making risk management a standing item on the board agenda.*

Towards the end of each year management may choose to provide a summary of the risk management activity throughout the year to the board. Such reporting can be fully considered by the board for its appropriateness and support the public disclosures that the board needs to make (see section 6).

The items covered in the summary report to the board should include:

- the processes that occurred throughout the year:
  - annual review and update of risk management policy (include a copy of the latest policy)
  - other appropriate risk management framework information
  - identification of material business risks (re-produce material from section 5.1 including risk profile and risk matrix)
  - a summary of the risk reporting of individual material business risks that occurred throughout the year.
- a suggested corporate governance statement for inclusion in the annual report
- two management statements based on the above information:
  - that management has designed and implemented an appropriate risk management and internal control system to manage the company's material business risk
  - that management has effectively managed (throughout the year) the material business risks.

The management summary outlined above can be provided verbally and be minuted or prepared as a written statement. The statement should be supported by appropriate material and completed around the same time as financial statements are being considered by the board.

**Action:**  
Complete combined Principle 7.3 and s295A signed certification by the CEO and CFO (Appendix G) and ensure this is supported by appropriate documentation.

**CEO/CFO signed certification on financial reporting risks**

Financial reporting risks relate to the processes and controls that support the preparation of reliable and accurate financial reports. They are viewed as a sub-set of material business risks and have special requirements attached to them. These requirements have not changed since the first version of the Principles.

The new recommendation is that the CEO (or equivalent) and the CFO (or equivalent) provide written assurance to the board that the risk management and internal control system is operating effectively to reduce financial reporting risks in all material respects. This requirement is designed to support the declaration required of the CEO and CFO by section 295A of the *Corporations Act 2001*.

Illustrative wording of this declaration to meet both the reporting requirements of Recommendation 7.3 and section 295A is set out in Appendix G.

A CEO and CFO should not sign this certification unless there is a reasonable basis of support. Doing nothing or just relying on the external audit process is generally considered insufficient. Often for small – mid cap companies their external auditor does not review and rely on financial reporting controls when forming their audit opinion on the financial statements.

Furthermore, outsourcing the finance function does not alleviate this responsibility as risk cannot be outsourced and in this circumstance management should undertake and document procedures to ensure the outsource provider has taken reasonable efforts to ensure the integrity of the financial reporting process.

**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.

Where the finance function is retained in-house, the CEO and CFO should ensure they have documented the key control considerations and why they believe they are working. It would be appropriate for a suitably worded internal memo to be prepared outlining what controls exist and what activities have been undertaken to ensure that these controls are working. The inclusion of the table below in this memo should facilitate this.

Other financial controls that small – mid cap companies should consider are

- accounting resources and IT systems
- segregation of duties (including dual cheque signatory requirement)
- key transaction processing systems
- implementation of Delegation of Authority Policy
- audit independence
- accounting advice process
- preparation of financial report itself (especially to ensure all key disclosures are included).

Management should consider providing this documentation to the board with the certification required above so that the board can review the appropriateness of the basis upon which the certification was made.

Account	Key controls	Operating effectively?
Material accounts based on the latest financial statement	<ul style="list-style-type: none"> <li>• key control 1</li> <li>• key control 2</li> </ul>	Operating effectively based on: <ul style="list-style-type: none"> <li>• management review</li> <li>• independent audit</li> <li>• etc.</li> </ul>
For example, Cash	Bank reconciliation	CFO has reviewed and signed off bank reconciliation
	Facility/lease agreements	CFO has reviewed and ensured appropriate disclosures are reflected in the financial statements

### **Key tips**

ASX Markets Supervision has flagged its intention to focus on Principle 7 reporting in its reviews. In light of this, areas to ensure you are across include:

1. ensure your company is aware that the Principle 7 is now different
2. check what you are really saying – concentrate on the quality of disclosure and avoid 'boilerplate' statements in your annual report or website
3. ensure you are doing what you are saying – check that disclosures are actually aligned with the reality of the risk management and oversight within the company
4. consider whether what you are doing is sufficient – do you have the right risk maturity for your company?

# 6. What to publicly disclose?

The purpose of reporting under Principle 7 is to provide meaningful information to investors about the company's risk management policies and system.

Increasingly, stakeholders look to companies to provide evidence of effective management of not only the financial risks but also other non-financial material business risks in such areas as community affairs, human rights, employment practices, health and safety and the environment.

Consistent with the philosophy of open disclosure and an 'if not, why not' regime, the Principles do not prescribe the content, format or style of the public disclosures required under Principle 7. It is the expectation that such disclosures are not 'boilerplate' and provide genuine insight into the risk management processes and management of material business risks within the company.

It does, however, require the disclosures to include these items:

1. on the company's website in a section clearly titled 'corporate governance':
  - a summary of the risk management policy.
2. in the corporate governance statement for the annual report:
  - disclose that the board has received the:
    - annual summary on risk management effectiveness referred to in section 5.3
    - assurance certification from the CEO/CFO for financial reporting risks.
  - any departures from the requirements set out in Principle 7.

To assist companies, in June 2008, the ASX Corporate Governance Council published *Revised Supplementary Guidance to Principle 7* on helpful and unhelpful disclosures. The helpful disclosure has been re-produced at Appendix H for your reference.

## Recommendation 7.4

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

## What disclosures are NOT required by Principle 7?

The following disclosures are NOT required by Principle 7:

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

However when companies consider the issue of material business risks, they need to be aware of their obligations under ASX Listing Rule 3.1 to immediately make an announcement to the market in relation to some or all their material business risks and/or changes to those risks, where the risk or change is likely to have a material impact on the price or value of a company's securities. The board will need to exercise their judgement when considering whether such detailed disclosure is required.

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

### Action:

Publish information in the governance section of an annual report and/or website (Appendix H)

# Frequently asked questions

---

This section is designed to provide answers to some of the common questions relating to risk management reporting and Principle 7.

## **What is the role of this guide?**

The role of this guide is to assist small mid cap companies to understand and implement an effective risk management system which will allow them to report positively against the recommendations in Principle 7. However a statement of reliance on this Guide in a corporate governance statement is no guarantee that ASX Markets Supervision will not take supervisory action against the company. ASX Markets Supervision will judge each corporate governance statement against the requirement in listing rule 4.10.3 to report against the recommendations in the Principles and will not be limited in its rights to take action based upon any references to this Guide or the accompanying seminars if, in ASX Markets Supervision's opinion, the statement does not comply with the requirements of listing rule 4.10.3.

## **What is the role of management in relation to risk?**

Refer Appendix D.

## **Can the board rely on the assurance given by management only?**

As mentioned in section 5.3 of this Guide, there is no recommendation within the Principles to require additional assurance. However, the board or management may request additional assurance if they so desire to ensure the accuracy of the reporting from management to the board and the operation of controls.

For small – mid cap companies, a peer review by an independent director often provides the required comfort over the risk management process and related controls. Other alternatives include using external providers to provide focussed 'internal audit-like' services.

## **What is the scope of risk management to be addressed under Principle 7?**

As mentioned in section 2 in this Guide, the scope of Principle 7 covers material business risks. Material business risks should not be seen purely from a financial perspective. Examples of material business risk categories identified in Principle 7 that could have significant reputational as well as financial impact:

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

## **What is the accepted frequency of risk management reporting to the board?**

The frequency of risk management reporting should depend on three key factors:

- complexity of the company and the risks it faces
- inherent risk of the environment in which it operates
- stakeholder and board expectations

Risk management reporting frequency should be appropriate to allow management to communicate any material changes to the company's risks as well as any major developments, losses and incidents or near misses accurately in a timely manner.

Aligning risk management reporting to existing board reporting can help improve the frequency and the quality of information reported. You should consider making risk management a standing board agenda item.

## **What are the risk standards that apply?**

Recommendation 7.2 under Principle 7 recommends that 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.

Principle 7 doesn't explicitly state or recommend a particular methodology to be applied; however it does make reference to the Australian/New Zealand *Standard for Risk Management* – ANZ 4360 at [www.standards.org.au](http://www.standards.org.au) and COSO Enterprise Risk Management – Integrated Framework, published by the Committee of Sponsoring Organisations of the Treadway Commission at [www.coso.org](http://www.coso.org).

#### **How can the board best work with management to set a framework for thinking about risk and setting our risk tolerance level?**

The efficient working of the board and management is crucial for the success of all companies. It is important to leverage the depth of experience of the directors as well as maintain an open, regular and transparent communication line between management and the non-executive directors.

Management of the company should work with the board to create an appropriate risk management policy which sets out the company's willingness to accept risk and therefore its risk tolerance. The risk management policy should also clearly outline how identifying, managing and thinking about risk will be integrated into existing strategy setting, planning, budgeting and performance reporting processes.

While the individual responsible for the overall risk management within the company can prepare the risk management policy, the senior management team and the board should actively discuss the policy to determine whether it accurately addresses shareholder expectations and the nature of the company's core business.

#### **How can the board begin viewing risk not just in terms of potential losses to mitigate, but also in terms of potential rewards for intelligent risk-taking?**

By incorporating risk identification into management's and board's decision making processes, both the downside and upside of the risks will be presented to increase certainty of the best outcome to the company. For example, when a proposition is presented to the board the management team needs to actively show that they have considered the risks associated with the proposition and created appropriate management plans to address the risks (i.e. to realise the likely benefits and reduce the chance of a loss/failure).

#### **How can the board move risk from a separate agenda item to something that is integral to all the board's decision-making about strategy, capital allocation, and even succession planning?**

Appropriate risk management needs to be explicitly expressed as part of the company's culture which should be regularly discussed within the company. By incorporating risk identification and discussion into existing board reporting and being considered as part of every decision or action it should soon become part of the company's culture.

#### **How should the board structure its responsibilities for risk oversight?**

The responsibility for risk is a responsibility of the full board of directors. However, the Principles endorse procedural items being handled by a committee, such as an audit and risk committee, with appropriate reporting to the main board.

However, given the nature of small – mid cap boards, the limited number of non-executive directors and the linkage between strategy and risk, it is often most efficient and effective for risk to be considered by small – mid cap companies at the main board level.

#### **How can the company best share information about risk among all board members without overwhelming directors?**

Focussing the board discussion on material business risks (not all risks) will help to ensure board's attention is directed towards the most critical issues. Incorporating risk reporting into existing performance and status board reporting can also help link risk management activity and effort to the company's broader goals and strategy and not overwhelm directors.

#### **What information needs to be disclosed in 2009 given that a company may only have recently started on the risk management journey?**

Principle 7 risk management disclosures should be provided for the full 12-month financial year. In this first year of application (to 30 June 2009), many small – mid cap companies may find themselves in the situation where they had not fully formalised their risk management and internal control system from the start of the financial year (1 July 2008).

In this circumstance, it is important that the company discloses what they have done and outline the risk journey they are on to improving and formalising their risk management and internal control system. If further actions are to be undertaken in the next financial year these should also be outlined to support this journey.

# Appendix A – Risk tolerance questionnaire

This high level questionnaire is intended to give an indication of the company's overall tolerance for taking and accepting risk as part of creating value.

	True	False	Unsure
Our company is eager to be innovative and to choose options offering potentially higher business rewards despite greater risks.			
Our company is prepared to invest for the best possible reward and accept the possibility of financial loss.			
Our company views new technology as a key enabler of operational delivery.			
Our company has high levels of devolved authority – management by trust rather than tight control.			
Our company is only willing to allocate limited resources to risk mitigation			
Our company has a tolerance for making decisions that are likely to bring scrutiny and attention of external stakeholders but where potential benefits outweigh the risks.			
Our shareholders are capable of tolerating increasing risk levels as part of generating additional shareholder value.			

#### Most answers 'true'

Your company appears to have a high tolerance for taking risks if they can be justified by greater rewards. Your stakeholders should understand this. Management should incorporate risk management into strategic planning and business decision making to understand and prioritise material business risks.

#### Most answers 'false'

Your company appears to be relatively risk averse and therefore should have strong risk management processes in place to ensure material business risks are understood and avoided or managed.

*Note: This questionnaire has been significantly simplified and is intended for the use of small to mid cap listed companies that are commencing implementation of a risk management process for the first time. It is intended to be used as a guide only, in order to provide direction about the risk process by the board and management so as to understand the expectations of each other using common language. The questionnaire should not be used for another purpose and should not be relied on solely without additional analysis undertaken.*



# Appendix B – Outline of a risk management policy

The following outlines the type of information that would usually form the basis for a set of policies and procedures for a common and systematic approach for managing risk across a company. This approach increases risk awareness, ensures the appropriate

management of risks, and makes the material business risks faced by the company transparent, thus enabling risks to be compared and aggregated and allows for appropriate risk oversight and reporting.

Prepared by: \_\_\_\_\_

Approved by: \_\_\_\_\_

Revision date: \_\_\_\_\_

Effective date: \_\_\_\_\_

## **Purpose:**

*Outline the purpose of creating a risk management policy and what it will achieve for the company.*

## **Scope:**

*Document the scope of the policy, where it applies (including subsidiaries, if applicable) and what risks should be covered by the policy.*

## **Policy:**

*Describe the key elements of a company's risk management policy:*

- *the objective and rationale for managing risk in the company*
- *clear links between the policy and the company's strategic plans and business plan*
- *guidance on the company's risk tolerance*
- *a statement on how risk management performance will be measured and reported*
- *details of the support and expertise available to help staff undertake effective risk management practices.*

*A company's risk management policy can also provide guidance to staff on the company's commitment to:*

- *integrating risk management principles into existing procedures and practices*
- *communicating the company's approach to managing risk*

- *coordinating the interface between risk management, compliance and assurance programs within the company*
- *incorporating risk management training into internal staff development programs.*

## **Definitions:**

*Provide relevant definitions and terms used throughout the policy and procedure documents.*

## **Procedure:**

### **Risk strategy and risk tolerance**

*Outline the company's tolerance for accepting risks and the strategy the company is intending to adopt to meet this requirement.*

### **Risk management requirements**

*Outline the steps that the company is intending to take to incorporate risk management into day to day operations as well as how it intends to make the risk management process sustainable.*

### **Assurance**

*Document what assurance process will be undertaken (internal and external) to determine that the risk management process and management of individual risks continue to operate effectively.*

### **Risk management roles and responsibilities**




*Outline responsibilities for managing risks at all levels of the company. Normally the following people will have some responsibility for developing a risk management process and managing risks on a day to day basis:*

- *Chief Executive/Board of Directors*
- *Audit and Risk Committee (if exists)*
- *Management team*
- *Supervisors (if applicable)*
- *Risk Manager (if applicable)*
- *Individual staff (if applicable).*

# Appendix C – Sample risk register

The following sample risk register may be used by companies to capture the information discussed in this guide.

1. Identify material business risks (refer section 5.1)			2. Prioritise the risks (refer section 5.1 and Appendix E)			3. Manage material business risks (refer section 5.2)		4. Report (refer section 5.3 and Appendix F)	
#	Risk description	Current controls	Effectiveness of current controls	Likelihood	Consequences	Risk level	Further management action required	Responsibility /timeframe	Status
1	<i>Describe each risk including potential consequences that may impact on the company if it eventuates.</i>	<i>List management controls currently in place to prevent or minimise the effect of risk occurring.</i>	<i>Consider the effectiveness of current controls in addressing the risk.</i>	<i>Determine the likelihood of risk occurring.</i>	<i>Determine the impact on company if it does occur.</i>	<i>Determine the overall risk level. The arrows may be used to track change in risk level since last report.</i>	<i>If risk level is too high or above company's risk tolerance, document additional management action required to reduce the risk level.</i>	<i>Allocate responsibility for each risk and specify timeframe.</i>	<i>Track the status of risk mitigation actions and report to the board.</i>

	<b>Legend</b> Risk level increased from last review
	Risk unchanged from last review
	Risk level decreased from last review

# Appendix D – Sample risk management roles and responsibilities

The list below identifies suggested accountabilities and responsibilities for managing risk in a company.

## Chief executive/Board of directors

- champion the company's governance and risk management processes
- determine the company's risk tolerance
- review recommendations from the company's audit and risk committee(s) (if exist) and determine future actions
- publicly report and make the necessary disclosures relating to risk as required by Principle 7.

## Audit and risk committee (if exist, otherwise reverts to the full Board of directors)

- oversee the risk management framework
- ensure the risk management framework is implemented and adopted
- review and approve the company's list of material business risks (risk profile) and risk treatment strategies
- monitor the implementation of the risk management program against the endorsed implementation strategy or plan
- confirm that the company's risk management process is continually maturing to reflect the changing environment and allows the company to identify and respond to emerging issues and risks
- receive reports from management on the effect of material business risks.

## Chief executive/senior management

- develop the company's strategic risk profile by identifying and prioritising material business risks
- review the company's risk profile periodically
- review and assess the current and planned approach to managing material business risks
- review and monitor the status of risk treatment strategies
- periodically report on material business risks to the board/audit and risk committee
- ensure the risk management framework is implemented across the different areas of operations.

## Managers and supervisors

- monitor the material business risks for their areas of responsibility
- provide suitable information on implemented treatment strategies to senior management to support ongoing reporting to the board
- ensure staff are adopting the company's risk management framework as developed and intended

## Risk manager (or equivalent)

- coordinate the implementation of the risk management framework, risk profile and treatment strategies
- facilitate, challenge and drive risk management development within the company
- report to the senior management, executive management and audit committee or board at regular intervals on the risk process (not individual risks).

## Individual staff

- recognise, communicate and respond to expected, emerging or changing material business risks
- contribute to the process of developing the company's risk profile
- implement treatment strategies within their area of responsibility.

# Appendix E – Risk matrix guidance

## Companies can apply the following risk matrix during the risk identification and prioritisation process.

The purpose of risk prioritisation is to determine the overall risk level for each material business risk identified by the company. To calculate the overall risk level companies need to assess the likelihood of the risk occurring and the magnitude of the consequences if the risk eventuates taking into consideration controls that are already in place:

- risk likelihood can be expressed in terms of probability of the risk event occurring and normally is represented on a scale of five from rare to almost certain. Likelihood should be considered within a defined period of time, for example annual planning period or five year strategic plan
- the consequences can also be represented on a five point scale from insignificant to critical/extreme. Consequences should be considered not just from a financial perspective but also take into account safety, environment, legal and reputational impacts.

Specific likelihood and consequence criteria should be set for each company individually.

The matrix below shows the relationship between likelihood and consequence ratings and various risk levels. Material business risks that fall in the sector coloured in blue usually represent risks that are possible or likely to occur and if they do they will have a significant impact on the company.



*For risks in this sector of the matrix, compare to the company's risk tolerance and consider reducing, transferring or accepting the risk (refer section 5.2)*

# Appendix F – Outline of an individual risk report

## Sample individual risk report

### Risk:

*[this should reflect the 'Risk Description' item in the risk register]*

### Management responsibility/risk owner:

*[e.g. Chief Executive Officer]*

### Report delivered to:

*[e.g. Audit Committee]*

### Date report delivered:

### Reporting frequency and no. of report in series:

*[e.g. Report No. 1 of 4.]*

### Focus and scope of this report:

*[report on any further management action required under the Risk Register, identify any actions taken/not taken, any outcomes or consequences of action, any events that have occurred in relation to the risk and any impact or change on the risk]*

### Action plan:

Objective	Activity	Owner due date	Status
<i>[key objectives impacted by this risk]</i>	<i>[key actions to manage this risk]</i>		<i>[in planning/in progress/delayed/completed]</i>

### Key controls mitigating the risk:

*[e.g. quarterly independent compliance review, insurance, etc.]*

### Assurances:

*[e.g., outcome of any independent party review]*

### Interdependent or related risks:

*[e.g. another risk linked with this risk]*

### References and related documents:

*[e.g. policy and procedure document]*

### Other comments or outcomes:

*Based on the above this material business risk is being managed effectively.*

### Signature:

*[Risk owner]*

### Date:

# Appendix G – Illustrative wording for CEO and CFO certifications

The following is an illustrative wording for the CEO and CFO certifications to meet the reporting requirements of both Recommendation 7.3 under Principle 7 and also satisfies s295A of the Corporations Act 2001, as extracted from the Deloitte/Group of 100 *Recognise and manage risk: A Guide to compliance with ASX Principle 7* (August 2008), Appendix 2:

## **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 H – Hypothetical helpful public disclosure example

The following has been reproduced from the *Revised Supplementary Guidance to Principle 7* (June 2008) issued by the ASX Corporate Governance Council. The full details of this supplementary guidance should be reviewed. Companies should also not simply reproduce the following.

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

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

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

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

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

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

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

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

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

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

*Detailed internal control questionnaires are completed by all major divisions and key finance managers in relation to financial and other reporting on a six monthly basis. These are reviewed by our senior finance team and our external auditors as part of our half-yearly reporting to the market and to achieve compliance with section 295A of the Corporations Act and Recommendation 7.3 of the ASX Corporate Governance Council's Corporate Governance Principles and Recommendations.*

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

*The Board also receives a written assurance from the Chief Executive Officer (CEO) and the Chief Financial Officer (CFO) that to the best of their knowledge and belief, the declaration provided by them in accordance with section 295A of the Corporations Act is founded on a sound system of risk management and internal control and that the system is operating effectively in relation to*

*financial reporting risks. The Board notes that due to its nature, internal control assurance from the CEO and CFO can only be reasonable rather than absolute. This is due to such factors as the need for judgement, the use of testing on a sample basis, the inherent limitations in internal control and because much of the evidence available is persuasive rather than conclusive and therefore is not and cannot be designed to detect all weaknesses in control procedures.*

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

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

The ASX Corporate Governance Council comments that *"This disclosure is considered helpful as it provides a comprehensive view on how the company approaches risk management and oversight. The disclosure also provides insights in relation to the risks in the industry in which the company operates"*.



# Appendix I – Process checklist to implementation

A checklist below has been included to assist the reader to report positively against the recommendations of Principle 7 in their annual reports.

Board meeting	Action	Has action been completed?	Status	Reference in the guide
Quarter one	Complete risk tolerance questionnaire			4.1
	Draft Risk Management Policy			4.2
	Approve Risk Management Policy			4.2
	Publish Risk Management Policy on the company website			4.2
	Review board charter and role descriptions to ensure accountability for risk is included			4.3
	Management and board to identify material business risks and document in the risk register in year and continue to reassess the full list of risks in consecutive years			5.1
	Allocate risk owners to critical risks			5.1
Quarter two	Manage material business risks			5.2
	Update the risk register or prepare individual risk reports and present to the board			5.3
Quarter three	Manage material business risks			5.2
	Update the risk register or prepare individual risk reports and present to the board			5.3
Quarter four (full year)	Manage material business risks			5.2
	Update the risk register or prepare individual risk reports and present to the board			5.3
	Prepare CEO/CFO certification			5.3
	Prepare a summary of the risk management activity throughout the year and present to the board (including effectiveness statement)			5.3
	Prepare annual report disclosure with respect to Recommendation 7.4 under Principle 7			6

# Appendix J – Useful references

**ASX Corporate Governance Council:**  
[www.asx.com.au/corporategovernance](http://www.asx.com.au/corporategovernance)

**Blakiston & Crabb Corporate Governance:**  
<http://www.blakcrab.com.au/>

**Deloitte ASX Principles:**  
[www.deloitte.com/au/corporate\\_governance](http://www.deloitte.com/au/corporate_governance)

**Deloitte Risk Intelligence:**  
[www.deloitte.com/RiskIntelligence](http://www.deloitte.com/RiskIntelligence)

**Group of 100:**  
[www.group100.com.au](http://www.group100.com.au)

**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)

**COSO Internal Controls and ERM models:**  
[www.coso.org](http://www.coso.org)

**AS/NZS 4360:2004 Risk Management:**  
[www.standards.org.au](http://www.standards.org.au)





## Contact us

### **Deloitte**

225 George Street  
Sydney, New South Wales  
Australia  
[www.deloitte.com.au](http://www.deloitte.com.au)

### **Craig Mitchell**

Tel: +61 (0) 7 3308 7400  
email: [cmitchell@deloitte.com.au](mailto:cmitchell@deloitte.com.au)

### **Alex Sidorenko**

Tel: +61 (0) 2 9322 7412  
email: [asidorenko@deloitte.com.au](mailto:asidorenko@deloitte.com.au)

### **Blakiston & Crabb**

1202 Hay Street  
West Perth WA 6005  
Australia  
[www.blakcrab.com.au](http://www.blakcrab.com.au)

### **Julie Athanasoff**

Tel: + 61(0) 8 9322 7644  
email: [jathanasoff@blakcrab.com.au](mailto:jathanasoff@blakcrab.com.au)

### **Dalveen Belyea**

Tel: +61 (0) 8 9322 7644  
email: [dbelyea@blakcrab.com.au](mailto:dbelyea@blakcrab.com.au)

### **ASX Markets Supervision**

20 Bridge Street  
Sydney, New South Wales  
Australia  
[www.asx.com.au](http://www.asx.com.au)