Risk management & internal control

Audit committees have an essential role to play in ensuring the integrity and transparency of corporate reporting.

The PwC Audit Committee Guide is designed to help members of the audit committee work through their maze of responsibilities in a practical manner.
Audit committees have an essential role to play in ensuring the integrity and transparency of corporate reporting.

The PwC Audit Committee Guide is designed to help members of the audit committee work through their maze of responsibilities in a practical manner.

**Financial reporting**
- Appropriateness of accounting policies
- Disclosure requirements
- Fairness and balance of MD&A/operating review
- GAAP conversion

**External audit**
- Appointment and remuneration
- Scope of work
- Independence requirements
- Significant audit findings/recommendations
- Reviewing the performance of external auditors

**Risk management & internal control**
- Understanding of key risk areas
- Effectiveness of controls
- Fraud risk

**Internal audit**
- Charter, authority and resources
- Scope of work
- Internal audit effectiveness
- Responses to internal audit recommendations

**Maintaining & measuring effectiveness**
- Training needs
- Maintaining financial literacy
- Annual performance evaluation of audit committee

**Communicating & reporting**
- Relations with management
- Updates and recommendations to the full board
- Reports to the board and shareholders

**Regulatory, compliance & ethical matters**
- Effectiveness of system for ensuring compliance with laws and regulations
- Code of conduct/ethics
- Whistleblowing

The guide consists of:
- Introduction
- Setting up the audit committee
- Financial reporting: Reviewing financial information
- Risk management & internal control
- Working with the external auditor
- Understanding internal audit
- Maintaining & measuring effectiveness
- Communicating & reporting
- Ethical, regulatory & compliance matters
- Compliance frameworks
- The audit committee’s role in ‘fit and proper’ requirements for financial services entities
- Materiality in audits

We hope you will find this guide of value to your important role. If you would like to provide any feedback, or if you need more information, call your usual PwC contact.
1. Understanding risk management and internal control

Risks are uncertain future events – both positive and negative – that have the potential to affect the achievement of a company’s goals and objectives. A common feature of successful companies is the ability to navigate the many risks and uncertainties they face in the pursuit of shareholder value.

Those companies successfully use strategies that help them:

- cost-effectively protect their exposure to events that have the potential to destroy shareholder value
- identify and seize opportunities to increase shareholder value through prudent risk-taking and a consideration of the balance between risk, growth and returns
- effectively control activities and processes towards the achievement of company objectives.

One of the factors that can help a company achieve these objectives is an effectively functioning risk management and internal control framework.

An effective framework

The three most commonly used sources of guidance on the elements of an effective risk management and internal control framework are the:

- Australia/New Zealand Standard on Risk Management (AS/NZS 4360) and accompanying handbooks
- Enterprise Risk Management Conceptual Framework (published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO)).
- Internal Control – Integrated Framework (also published by COSO).

All three sources provide a useful description of many risk management and internal control concepts, and are a useful point of reference when considering a company’s risk management and internal control framework.

However, they are necessarily conceptual in nature, and require considerable judgement, interpretation and customisation before being successfully applied within a company.

For example, COSO’s Enterprise Risk Management Conceptual Framework (which encompasses internal control) describes enterprise risk management as:

“...a process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”

The framework identifies eight interrelated components, which, integrated with existing management processes, help an organisation achieve strategic, operational, compliance and reporting objectives.
1. Understanding risk management and internal control

The eight COSO risk management components

Internal environment – Management sets a philosophy regarding risk and establishes a risk appetite. The internal environment sets the basis for how risk and control are viewed and addressed by an entity’s people. The core of any business is its people – their individual attributes, including integrity, ethical values and competence – and the environment in which they operate.

Objective setting – Objectives must exist before management can identify events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives, and that the chosen objectives support and align with the entity’s mission and that they are consistent with its risk appetite.

Event identification – Potential events that might have an impact on the entity must be identified. Event identification involves identifying potential events from internal or external sources that affect the achievement of objectives. It includes distinguishing between events that represent risks, those representing opportunities and those that may be both. Opportunities are channelled back to management’s strategy or objective-setting processes.

Risk assessment – Identified risks are analysed to form a basis for determining how they should be managed. Risks are associated with objectives that may be affected. Risks are assessed on an inherent and a residual basis, with the assessment considering risk likelihood and impact.

Risk response – Personnel identify and evaluate possible responses to risks, which include avoiding, accepting, reducing and sharing risk. Management selects a set of actions to align risks with the entity’s risk tolerances and risk appetite.

Control activities – Policies and procedures are established and executed to help ensure the risk responses management selects are effectively carried out.

Information and communication – Relevant information is identified, captured and communicated in a form and timeframe that enables people to carry out their responsibilities. Information is needed at all levels of an entity for identifying, assessing and responding to risk. Effective communication also occurs in a broader sense, flowing down, across and up the entity. Personnel receive clear communications regarding their role and responsibilities.

Monitoring – The entirety of enterprise risk management is monitored, and modifications made as necessary. In this way, it can react dynamically, changing as conditions warrant. Monitoring is accomplished through ongoing management activities, separate evaluations of enterprise risk management, or a combination of the two.

The design of a risk management and internal control framework must address how each organisation makes decisions in key areas such as strategy, investment and financial management. What works well in one industry may not necessarily be effective in another, and individual companies will often have quite legitimate differences of approach according to factors such as:

- industry
- company size
- organisational model (ie centralised vs decentralised)
- governance structures in place within the company
- organisational culture and management operating style
- existing business planning, investment decision-making and performance monitoring processes.
2. Responsibilities of the board and the audit committee

Responsibility for the effective management of risk, and control of a company’s operations, lies with a company’s CEO and management team. To fulfil their oversight responsibilities, however, boards need to be certain that those responsibilities are carried out proactively, systematically and effectively.

The board’s responsibilities with respect to risk management and internal control can be summarised as follows:

1. Establish a ‘tone at the top’ that promotes a risk-aware culture
2. Agree with management the company’s risk appetite
3. Be informed about the company’s risk profile as well as the measures that management is taking in relation to significant risks and uncertainties
4. Ensure that the company has appropriate processes for identifying, assessing and responding to risks in accordance with the organisation’s risk appetite, and that those processes are operating effectively
5. Ensure that the company’s activities are effectively controlled so that management’s risk responses and policies are carried out as planned towards the achievement of strategic, operational, compliance and reporting objectives.

While establishing an appropriate ‘tone at the top’, agreeing on the company’s risk appetite and monitoring the strategic risks facing the company are responsibilities that will typically remain with the board, many of the other responsibilities with respect to risk management and internal control are often delegated to the audit committee (and in some cases to a separate risk management committee).
## 2. Responsibilities of the board and the audit committee

### The audit committee’s responsibilities and how to meet them

<table>
<thead>
<tr>
<th>Audit committee responsibility</th>
<th>Points to consider</th>
</tr>
</thead>
</table>
| To be informed about the company’s risk profile | • Does management have a structured process for periodically identifying, assessing and reporting its risk profile and associated management activities to the audit committee?  
• If so, is the audit committee satisfied that process provides a complete picture of the company’s risk profile?  
• Does the audit committee charter describe the types of risks it is required to monitor and which management will report on? In many cases this list will include:  
  – risks associated with the breakdown in key business processes (in particular, financial reporting and financial management processes)  
  – fraud-related risks  
  – risks of non-compliance with key laws and regulations  
  – business continuity and disaster preparedness.  
• Does the audit committee’s program of meetings monitor the evolution of significant risks and management’s action plans? |
| Oversight that risk-taking is in accordance with the company’s risk appetite | • Does the audit committee understand the key components of the company’s risk management framework? What processes, accountabilities and influencers of organisational behaviour are key to the way the organisation manages risk?  
• How does the audit committee obtain assurance that those components are functioning as intended? Is it provided with KPIs for the operation of the framework?  
• What processes help to ensure that management decision making incorporates a sufficient consideration of risk and uncertainty, and how does the audit committee obtain assurance that management is operating effectively?  
• How does the audit committee obtain assurance that the information it receives is complete, reliable and accurate?  
• How does the audit committee form a view as to how the culture of the organisation influences the management of risk and uncertainty?  
• What information does the audit committee have about risk events that have occurred and are within its sphere of authority? |
| Oversight of the company’s state of internal control | • To what extent does the audit committee understand what the key business processes are and where tight internal control is required?  
• Does the audit committee receive reliable information on any incidents of fraud or major control breakdowns?  
• Does management make any representations to the audit committee about the effectiveness of internal control in key business processes? To what extent has management made sufficient enquiries to support these representations?  
• Does the audit committee receive sufficient independent feedback on the operation of key controls from the company’s internal and external auditors?  
• How does the audit committee monitor and follow up management’s implementation of any corrective actions for control weaknesses? |
3. Applying ASX Corporate Governance Council Principle 7

**Within Australia, ASX-listed companies are required to consider and publicly state the extent to which they have chosen to adopt the recommendations of Principle 7: Recognise and manage risk of the ASX Corporate Governance Council’s Principles of Good Corporate Governance and Best Practice Recommendations. The recommendations outlined in Principle 7 are:**

**Recommendation 7.1**
Companies should establish policies for the oversight and management of material business risks and disclose a summary of those policies.

**Recommendation 7.2**
The board should require management to design and implement the risk management and internal control system used to manage the company’s material business risks and report to it on whether those risks are being managed effectively. The board should disclose that management has reported to it as to the effectiveness of the company’s management of its material business risks.

**Recommendation 7.3**
The board should disclose whether it has received assurance from the chief executive officer (or equivalent) and the chief financial officer (or equivalent) that the declaration provided in accordance with section 295A of the *Corporations Act 2001* is founded on a sound system of risk management and internal control and that the system is operating effectively in all material respects in relation to financial reporting risks.

**Recommendation 7.4**
Companies should provide the information indicated in the guide to reporting on Principle 7.

While the ASX has intentionally not prescribed the way companies should meet these guidelines, guidance has been developed by the G100 (the Group of 100, representing Australia’s senior finance executives) in its publication Guide to Compliance with ASX Principle 7 'Recognise and manage risk'.
### 3. Applying ASX Corporate Governance Council Principle 7

**Applying the Principle 7 recommendations**

The following table sets out some matters for the audit committee to consider in relation to the Principle 7 recommendations.

<table>
<thead>
<tr>
<th>What to ask</th>
<th>Who to ask</th>
<th>What to look for in response</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Recommendation 7.1 – Risk management policy</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Do we have a risk policy and is it publicly available on our website? | Company secretary | The policy describes the following elements:  
- the roles and responsibilities of the board, audit committee, management and the internal audit function  
- the key elements of the company’s risk management system  
- the nature of risks that the company’s risk management system focuses on  
- a requirement that the board review, at least annually, management’s implementation of the risk management system  
- the frequency with which the audit committee must review the policy. |
| **Recommendation 7.2 – Chief executive and chief financial officer’s statement to the board** | | |
| What is the scope of the statement and does it satisfy the audit committee’s expectations? | CEO/CFO | The majority of companies have chosen to limit the CEO/CFO statement to the effectiveness of internal control over the financial reporting process.  
However, in some companies the audit committee has asked that management (often broader than just the CEO/CFO) comment on the effectiveness of risk management, internal compliance and control in additional areas (eg legislative compliance, OH&S). |
| What is the breadth of operations covered by the statement? | CEO/CFO | The audit committee should ensure that it understands and is comfortable with the scope of the sign-off provided.  
Does it cover the operation of controls in all subsidiaries, material joint ventures and material associates (including outsourced service providers)?  
Does it cover the operation of controls during the full year as opposed to a point in time such as the financial year-end? |
| What steps have the CEO/CFO taken to support their statement? Has their evaluation been sufficiently robust? | CEO/CFO | Is the statement supported by a systematic and comprehensive evaluation process which included:  
- a consideration of risk management, internal compliance and control against an established set of criteria such as those of the COSO framework  
- a consideration of the effectiveness of the design of internal controls  
- remediation of weaknesses identified  
- testing of the operating effectiveness of key controls?  
Is there evidence that the CEO and CFO have actively reviewed and understood the results of the evaluation rather than passively accepting a recommendation provided by staff?  
How do the results of the evaluation compare with the findings of internal and external audit during the year?  
Have material weaknesses been identified elsewhere that have not been identified by the CEO/CFO in their statement? |
### 3. Applying ASX Corporate Governance Council Principle 7

<table>
<thead>
<tr>
<th>What to ask</th>
<th>Who to ask</th>
<th>What to look for in response</th>
</tr>
</thead>
</table>
| **Recommendation 7.3 – Management** | Management | The majority of companies have chosen to limit management’s statement to the effectiveness of internal control over the financial reporting process only. The audit committee should ensure that it understands and is comfortable with the scope of the sign-off provided. Is the statement supported by a systematic and comprehensive evaluation process which included:  
  • a consideration of risk management, internal compliance and control against an established set of criteria such as those of the COSO framework  
  • a consideration of the effectiveness of the design of internal controls  
  • remediation of weaknesses identified  
  • testing of the operating effectiveness of key controls? |
| What is the scope of the statement and does it satisfy the audit committee’s expectations? | Management | Does it cover the operation of controls in all subsidiaries, material joint ventures and material associates (including outsourced service providers)? Does it cover the operation of controls during the full year as opposed to a point in time such as the financial year-end? |
| What is the breadth of operations covered by the statement? | Management | Where the company has made a conscious decision to not adopt one of the recommendations under Principle 7, has it clearly stated its reasons in its annual report? |
| **Recommendation 7.4 – Public disclosure** | Company secretary | If the CEO/CFO statement identifies one or a number of material weaknesses in internal control, this represents a departure from Recommendation 7.2 and should be disclosed in the annual report. |
| Has the company disclosed any departures from the recommendations of Principle 7 in the corporate governance section of its annual report? | Company secretary | Is the description of the system of risk management, internal compliance and control consistent with the scope of the statement provided by the CEO and CFO? If it covers a broader group of risks than does the statement, is there a possibility that there will be an expectation gap on the part of readers? |
| In the annual report, how has the company described its system of risk management, internal compliance and control? | Company secretary | Confirmation that the risk policy is on the corporate governance section of the website. |
| Has the company placed a copy of its risk policy in the corporate governance section of its website? | Company secretary | |