Deloitte.

GROUP OF 100

ASX Corporate Governance Council Principle 7
Recognise and manage risk

Better Practice Guide 3rd Edition
January 2015

Know the worth of risk.

Preface

Good corporate governance is essential for efficient capital markets and investor confidence.

The ASX Corporate Governance Council's Corporate Governance *Principles and Recommendations* set the benchmark for good corporate governance practices in Australia.

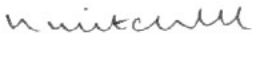
The Group of 100 is committed to assisting its members achieve good governance outcomes by developing a guide to better implement the ASX Corporate Governance Council's *Principles and Recommendations*.

This Better Practice Guide prepared by the G100 and Deloitte is the third edition and follows the release in March 2014 of the revised ASX Corporate *Governance Council Principle 7: Recognise and manage risk*.

The purpose of the Guide is to provide an overview of the key changes to Principle 7, and an understanding of the attributes of effective risk management and how it can help drive performance and top quality corporate governance.

It is critical that a company's risk management and internal control framework is tailored to its individual circumstances. Accordingly, this Guide does not specify or adopt a particular model or approach, but rather brings together useful local and global concepts and ideas to consider when implementing or reviewing the effectiveness of a company's risk management framework.

We recommend this publication to Group of 100 members and other interested parties as a valuable reference to facilitate better practices for complying with Principle 7.



Neville Mitchell
President
Group of 100

Peter Matruglio
National Lead Partner, Risk Transformation
Deloitte

Transitioning to new *Principle 7*

The following table provides a guide for listed entities to consider about new Principle 7. It is sourced from the recommendations of Principle 7, the associated commentaries and relevant presentations provided by the ASX Corporate Governance Council in May and June 2014.[1]

Key considerations		Change from the 2nd Edition	Better Practice Guidance (page)
Rec 7.1 Committees to oversee risk	• If you have, or intend to have, a committee or committees to oversee risk, check its composition and whether you have disclosed its charter (Rec 7.1(a)) • If you don't have a risk committee, articulate the processes the Board employs to oversee your risk management framework to satisfy itself that it is sound (Rec 7.1(b)) Listed entities which don't have a risk committee should consider how their disclosures about their risk management framework will read to investors and whether the framework should be upgraded.	Modified	Page 14
Rec 7.2 Annual review of risk management framework	• If you haven't already, articulate your risk management framework and review process • Consider how your disclosures about your entities risk management framework review process will read to investors and whether the review process should be upgraded • If you haven't already, institute a process for the Board or a committee of the Board to review your risk management framework at least annually to satisfy itself that it continues to be sound • Disclose if such review has taken place during the relevant reporting period in your annual report website.	Modified	Page 18
Rec 7.3 Internal Audit	• If you have an internal audit function, disclose how the function is structured and what role it performs • If you don't have an internal audit function, disclose the processes you employ for evaluating and continually improving the effectiveness of your risk management and internal control processes • Consider your disclosures and whether you should upgrade your internal audit function/processes	New	Page 20

1 Sources: ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 3rd edition; Kevin Lewis, ASX/ ASX Corporate Governance Council Developments, May – June 2014; Kevin Lewis, ASX Corporate Governance Council, Transitioning to the third edition of the Principles and Recommendations – Presentation to the GIA, June 2014

Key considerations		Change from the 2nd Edition	Better Practice Guidance (page)
Rec 7.4 Economic, Environmental and Social sustainability risks	• Consider whether you have a material exposure to sustainability risks (noting the definitions of 'economic sustainability', 'environmental sustainability, 'social sustainability' and 'material exposure' in glossary and footnote 38 of third edition) • Ensure your risk management framework and review process addresses sustainability risks including identifying and measuring material exposures • If your organisation has material exposure, disclose those risks and how you manage, or intend to manage them • If no material exposure exists, state that no material exposure exists and consider explaining the basis of your assessment • Rec 7.4 does not require you to publish a sustainability report – but, if you do, you can meet Rec 7.4 requirements by cross-referring to that report • You can also meet Rec 7.4 by cross-referring to the relevant sections in your operating and financial review if they appropriately disclose the material risks and how they are managed.	New	Page 23
Rec 4.2 CEO/CFO Declarations	Before approving financial statements for any financial period (including half/ quarter year), the Board should receive a declaration from the CEO and CFO that, in their opinion: • The financial records of the entity have been properly maintained • The financial statements comply with the appropriate accounting standards and give a true and fair view of the financial position and performance of the entity • The opinion has been formed on the basis of a sound system of risk management and effective internal controls • The institution of processes to ensure CEO/CFO declarations are tabled at Board meetings that approve financial statements.	Modified (formerly Rec 7.3 in 2nd edition)	Page 25

Contents

Introduction

Background

The ASX Corporate Governance Council Principles and Recommendations were initially introduced in 2003 and subsequent revisions were made in 2007 and 2010.

As a result of the events that occurred both before and during the Global Financial Crisis, a number of jurisdictions have adopted new legislation to tighten corporate governance codes.

Following a comprehensive review and consultation process, the third edition of the Principles and Recommendations was released on 27 March 2014 and took effect for a listed entity's first full financial year commencing on or after 1 July 2014.[2]

The purpose of reporting under Principle 7 is to provide meaningful information to investors about the entity's risk management framework. Stakeholders expect companies to provide evidence of effective management regarding financial risks as well as other non-financial material business risks.

Consistent with open disclosure and an 'if not, why not?' regime, the principles do not prescribe the content, format or style of the public disclosures changes under Principle 7.

Key Changes to Principle 7 Recommendations – Recognise and Manage Risk

The recommendations on risk (Recommendations 7.1 – 7.4) have been substantially enhanced to reflect the lessons of the Global Financial Crisis and other developments. The ASX Corporate Governance Council encourages all listed entities to review the enhanced risk recommendations carefully and to consider whether they need to upgrade their corporate governance practices[3]. Principle 7, its recommendations and commentary is reproduced in full in Appendix A to this guide.

- **Recommendations 7.1 and 7.3** allow listed entities to adopt and report alternative practices in corporate governance
- **Recommendation 7.2** advocates that the Board, or its committee, should review the entity's risk management framework at least annually to satisfy itself of its effectiveness
- **Recommendation 7.3 of the third edition** is a new recommendation where a listed entity should disclose whether it has an internal audit function, how it is structured and what role it performs. If an entity does not have an internal audit function, it should disclose the fact and the processes used to evaluate and improve the effectiveness of its risk management and internal control processes.

  The CEO/CFO certification of financial statements from the 2nd edition has been upgraded and moved to recommendation 4.2 in the 3rd edition.

  The revised recommendation 4.2 now states that before the Board of a listed entity approves the entity's financial statements for a financial period, it should receive a declaration from the CEO and CFO that, in their opinion, the financial records of the entity have been properly maintained, and that the financial statements comply with the appropriate accounting standards.

  The financial statements should also give a true and fair view of the financial position and performance of the entity and that, in the opinion of the CEO and CFO, the statements have been formed on the basis of a sound system of risk management and effective internal control.

  Unlike recommendation 7.3 in the second edition, this will apply to financial statements for any reporting period (including half yearly and quarterly) not only to year-end financial statements.

2 *http://www.asx.com.au/documents/asx-compliance/cgc-principles-and-recommendations-3rd-edn.pdf*

3 *http://www.asx.com.au/documents/asx-compliance/cgc-communique-march-2014-final.pdf*

- **New Recommendation 7.4** regarding increasing focus on economic, environmental and social sustainability risks.

  This recommendation has arisen in response to increasing focus by investors and the potential impact these risks pose to a listed entity's ability to create or preserve value. It is modified from Principle 3 from the second edition – 'act ethically and responsibly'.

  In order to meet this recommendation listed entities should consider:
  - Ensuring the risk management framework and review process addresses sustainability risks, including assessment of material exposures
  - Providing disclosure of those risks - where material exposures to sustainability exists - including how they are managed, or intended to be managed
  - Disclosing the process to assess the risk in the unlikely case where there is no material exposure to sustainability risks

This recommendation does not require the entity to publish a sustainability report.

Cross referencing the existing sustainability report or relevant sections in the Operating and Financial Review (prepared in accordance to ASIC Regulatory Guide 247) is permitted. Where this disclosure approproiately covers sustainability risks, it may also meet Recommendation 7.4 requirements.

The key new terms introduced in this recommendation[4] include:

Economic sustainability – the long term ability of a listed entity to continue operating at a particular level of economic production.

Environmental sustainability – the long term ability of a listed entity to continue operating in a manner that does not compromise the health of the eco-systems in which it operates.

Social sustainability – the long term ability of a listed entity to continue operating in a manner that meets accepted social norms and needs.

Material exposure – the real possibility that the risk in question could substantively impact the listed entity's ability to create or preserve value for security holders over the short, medium or long term.

4 *ASX Corporate Governance Council, Footnote 38 and Glossary, ASX Corporate Governance Principles and Recommendations 3rd edition.*

Better Practice Guide

General Principle – A listed entity should establish a sound risk management framework and periodically review the effectiveness of that framework.

This Guide is designed to provide stakeholders including Board members, CEOs, CFOs and risk managers with concepts which they can leverage as they further refine or assess the effectiveness of their risk management frameworks.

This section is structured in a question and answer format to enable readers to form a view regarding factors to consider when reviewing, answering, or posing frequently asked questions regarding the effectiveness of risk management frameworks.

What are the potential risks that can destroy shareholder value for listed entities?

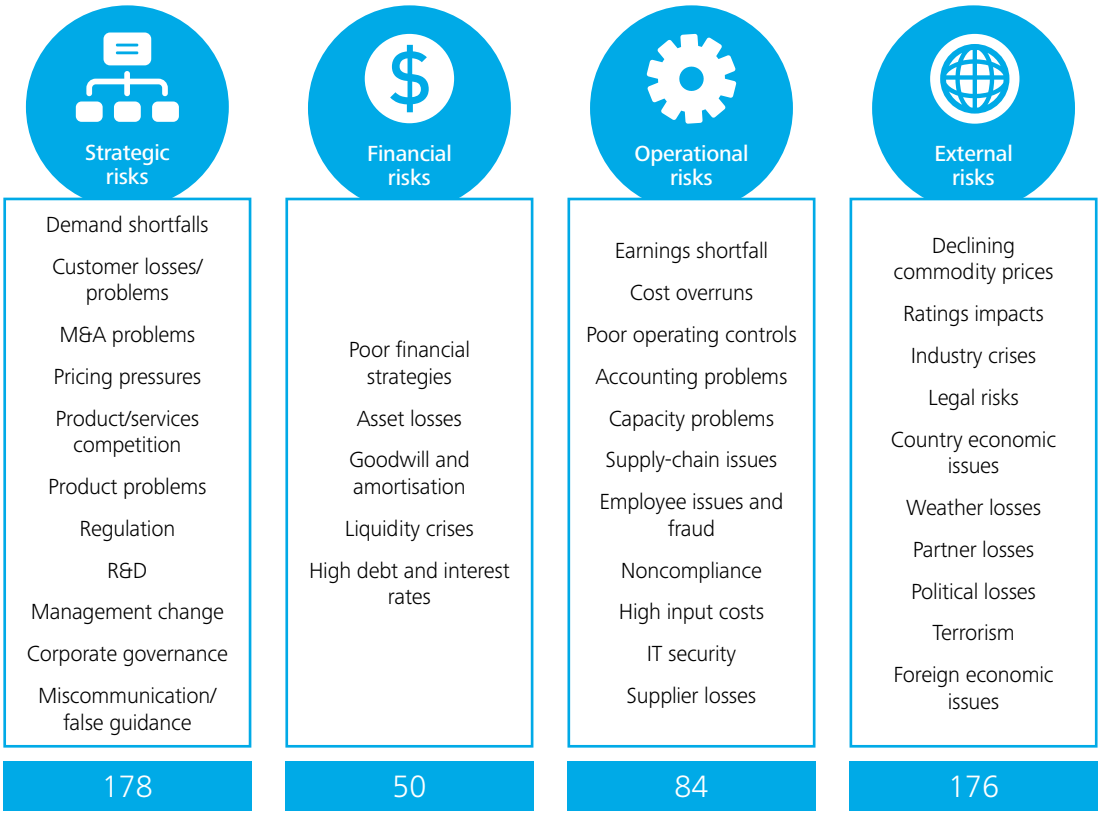
Better Practice Guidance

A listed entity's market capitalisation can be adversely impacted by both internal and external issues. Stakeholders should satisfy themselves that their company's risk management framework assists the entity develop an understanding of those risks that can lead to sharp falls in market capitalisation and what actions are necessary to protect that capital.

Recent global research[5] by professional services firm Deloitte found that during the last decade, 38% of companies in the MSCI Global 1000 index experienced 20% loss or more in market capitalisation in a period of 20 days or less. Two percent of those companies experienced market capitalisation losses of more than 50%. These significant losses are termed 'value killer events'.

Deloitte identified 36 contributing risk factors that drove these 142 distinct loss events. They are divided into four broad categories – strategic, financial, operational and external.

Four broad categories of risk and their frequency across 100 public companies with largest value drops[6]



Source: Deloitte

5 Deloitte, The value killers revisited: A risk management study, 2014

6 Assignments do not sum to 142 because loss events can be described by more then one category

In addition six risk themes were found to have destroyed the most shareholder value:

Black swans: High-impact, low-frequency events are the biggest threats to value. Large industry or economic events, such as the credit crisis or Eurozone crisis, created the greatest value lost over the last five years. These events expose a company's biggest strategic, operational and financial weakness, which can lead to further loss of shareholder value.

Ecosystems: The study reveals nearly three quarters of major loss events occurred through the ecosystem of related and interdependent risks. While a black-swan event may trigger significant value loss, its magnitude is often amplified by a variety of risk interdependencies across the company. Interdependent risks were the key driver of value losses in the first report and the latest research reaffirms the importance of considering risk events, in terms of their relationship to other events and ability to escalate substantial value loss.

Systemic risk: This risk was identified across many companies that were on the brink of collapse. Interdependencies within the financial services industry, other industries and companies dependent on financial services, made it critical to consider events and risks outside a company's core industry, but still within its ecosystem of critical resources.

Liquidity risk more salient: The financial downturn made real or perceived weaknesses in a company's balance sheet, and the potential inability to access capital, a more salient driver of value losses. Since the downturn, highly leveraged companies without sufficient liquidity reserves were at greater risk of value loss than comparable firms with less leverage. In the face of rising costs and slowing demand, lack of liquidity was often a critical constraint on the company and a driver of value losses.

Unsuccessful M&As: Unsuccessful M&A deals can be 'value killers' for many different reasons. Deals can go bad because of incorrect valuations before the deal, failure to complete an announced deal, changed economic circumstances after the deal, or failure to capture anticipated synergies, or effectively execute post-merger integration.

Culture, compensation and fraud risks: These risks arise when a company's culture and compensation plans create incentives for fraud or encourage employees to increase the risks that are assumed by a company.

While risks cannot be eliminated, companies can be better prepared to manage them. Scenarios and models can be built and embedded into risk management and business planning frameworks to explore how companies will manage when confronted with a value-killer event, especially, black swans. Companies can stress-test their capacity to respond to different scenarios where a bundle of events, mutually related or unrelated, occur at the same time.

The diagram below highlights challenges and considerations for addressing, and possibly pre-empting, potential events that can destroy shareholder value.

Key findings – Drivers of value loss

Culture and compensation risks

Challenge	Consideration
Incentive programs that reward short-term performance may create **unsustainable models of profit and companywide risks**.	How compensation and culture can **impact risk** taking by the company. Does it encourage risk taking **within or outside** the bounds of the **company's risk appetite**?

High-impact, low-frequency risks

Challenge	Consideration
Unexpected **'black swan'** events often caught companies by surprise, leading to value-killer losses.	Deploying broader **scenario planning and stress tests** to envision and plan for the consequences of a **broad range of risks** and rare events.

M&A risks

Challenge	Consideration
M&A can sometimes **fail to deliver the anticipated value**.	The viability of the M&A deal to **deliver anticipated returns under different and stressed economic scenarios**.

Correlated and interdependent risks

Challenge	Consideration
Almost 90% of the companies suffering the **greatest losses in value were exposed to more than one type of risk.** In most cases, an event exposed one major weakness that cascaded through the organisation.	Not looking at risks in isolation, and **construct scenarios to assess what could go wrong** in confronting the event and subsequent events across an enterprise and the ecosystem. Identify and evaluate buffers that help **mitigate against cascading risks**.

Liquidity risks

Challenge	Consideration
The global **financial crisis** made liquidity risk more salient and **increased the cost of capital** to those with high leverage and low ratings.	Current **liquidity and cash reserves,** and stress test the ability to **navigate a future credit crisis.** Work to ensure sufficient lines of credit from traditional and alternate sources of capital.

How can the Board of a listed entity identify the main internal and external risk sources that could adversely affect the entity's prospects in the future?

Better Practice Guidance

Under the Corporations Act[7] a listed entity established in Australia is required to include in its directors' report a discussion of the main internal and external risk sources that could affect the entity's prospects for future financial years.

To do this more effectively, companies are starting to formalise the following new practices:

Dynamic risk assessment and monitoring

As the business environments become more complex, and evolve faster, internal and external risks should be monitored with the same dynamism.

While the annual formal risk assessments continue to be the norm for some companies, other companies are increasing their frequency to reflect the internal and external conditions. In some cases, these periodic assessments are being enhanced and supplemented through the use of advance data analytical analysis of the underlying information maintained in an entity's existing management and financial systems. The purpose of these analytical reviews is to understand if there are any significant, previously unidentified risk trends or indicators which had not been previously incorporated into an entity's risk assessments. While technology can play a big role in an improved risk identification and assessment initiative, this needs to be supported by processes and a team that can interpret the data.

Strategic risk management

In a Forbes Deloitte global survey of more than 300 major global companies with revenues in excess of US$1 billion, conducted in 2013[8], two-thirds of the surveyed companies reported that their Boards and/or Board Risk Committees provide oversight of their strategic risks.

Strategic risks are risks that affect or are created by an entity's business strategy and strategic objectives.

The top strategic risks for companies include:

- **Company reputation** and the fallout from reputational damage
- **Emerging technologies** such as social media and mobile applications which increasingly are able to disrupt business models
- **Human capital** and the **innovation pipeline** which are expected to be the top strategic assets in which businesses will need to invest in the future.

The study suggests that companies should consider a broader set of risks and strategic assets – and include people, intellectual property, customers, and marketing efforts. These risks and assets are much more difficult to measure, capitalise on, and hedge against. They demand a much more systematic and sustained approach to monitoring and managing risk.

The implication is that there will be an increased focus on gathering data from customers, bloggers, information trend setters and marketplace and security analysts. It will also require learning from other companies and industries. Such sources may provide an emerging view of threats which are often not detected through traditional means.

7 ASX Principle 7 Recommendation 7.1 commentary refers to Section 299A of the Corporations Act and paragraph 61 of ASIC Regulatory Guide

8 Deloitte, Exploring Strategic Risk: A global survey. This study is a joint effort by Deloitte and Forbes Insights. The global survey included more than 300 respondents from the Americas, EMEA, and Asia/Pacific. Nearly all respondents were C-level executives (263), board members (22) or other risk executives (21). Surveyed companies came from all five major industry sectors (consumer/industrial products, life sciences/ health care, technology/media/telecommunications, energy and financial services), and all had annual revenues in excess of US$1 billion (or the equivalent)

How can good risk management practices help to protect established value and assist in identifying and capitalising on opportunities to create value?

Better Practice Guidance

Shareholder value is mainly driven by sustained positive returns on capital employed, and factors such as operating costs and taxes. The figure below shows how these drivers are impacted by specific forces and market conditions affecting a company.

Forces impacting shareholder value

Shareholder value

	Operating income	Operating costs	Risk and capital	Expectations
Specific forces	• Product and service offering • Funding costs.	• Technology • Human resources • Other costs.	• Strategic risk • Market, credit, liquidity and insurance risk • Operational risk • Regulatory risk • Other risk.	• Shareholders • Regulators • Clients/customers • Ratings agencies • Business conditions • Suppliers.
Specific market conditions	• Speed to market • Competitive pressures • Barriers to entry.	• Need to invest wisely in IT continues, as does the competition for talent • Competitors continue to improve their operating efficiencies and reduce costs.	• Regulations place increasing constraints on capital • Higher risks drive the need for more timely information and ad-hoc analysis of aggregate exposures and risk interdependencies.	• Shareholders seek improved/stable ROE and ROI • Regulators increase their scrutiny and ad-hoc requests • Rating agencies/ third parties scrutiny of risk management processes.

Pursuing shareholder value requires entities to focus simultaneously on external expectations, including regulatory requirements, and improving business management and risk management.

In the past, most company responses to external changes, economic indicators, shareholder demands and risk have been siloed. Although centred on risk, business models and operating models have typically not been explicitly aligned to risk management frameworks and practices.

Business units and functional areas viewed risk as the sole responsibility of the risk management function rather than inherent to their activities.

Improving risk management requires thinking on how siloed and ad hoc responses can be more effectively integrated across the company. Incorporating risk management into the conduct of business, by embedding it into the daily activities of employees, is one way to achieve this. It will strengthen both the management and governance of risk, and that of capital, operations and IT infrastructure.

An aligned company acknowledges both business unit and overall return on investment objectives, and the risk profile required to achieve those objectives. In this way operational risk management and risk governance policies, practices, roles and responsibilities will be aligned. The risk management function then supports each business to operate within agreed risk limits, actively and proactively managing the risks needed to meet return objectives.

Recent research[9] has identified four cornerstones which highlight cross-functional, risk-related elements and activities. When effectively co-ordinated, they can assist a company to effectively embed risk management into their organisation. These are:

Strategy: Strategy puts the company's vision and mission into action. Capital is allocated based on strategically selected risk-reward trade-offs, risk capacity, risk appetite, and desired risk profile. The executive team should consider the risks *of* and *to* the strategy and work with risk management and governance infrastructures to support the business model and capital allocation.

Governance and Culture: Governance ensures that strategies are executed properly and are aligned to risk and business strategy. Culture embodies the shared values, principles, and beliefs that guide the company. Together, governance and culture set the expectation for risk, enabling people to discern what is acceptable and unacceptable even when it is not explicitly addressed by policies and procedures. When considering governance and culture, the executive team might assess the company's level of risk intelligence, its risk management and governance frameworks, and its risk governance operating model.

Business and Operating Model: The business model defines economic relationships between the company and its customers, suppliers, investors, and other stakeholders. The operating model structures the ways activities are conducted with these stakeholders. Risk should be managed by clearly defining accountabilities, authority, and decision rules at all levels. Handoffs between business risk and control functions need to be well defined. Both business and operating models require standardised structures, processes, and controls for shared and outsourced services, as well as for business units and support functions.

Data, Analytics and Technology: Management should determine the key data required for insightful risk management and oversee the development of a data management and sourcing strategy. Facilitating the integration of finance and risk data also enables common and reconciled risk and compliance reporting. Business units need near real-time processing and reporting of aggregated data to monitor volatile market risks.

An enterprise risk data and architecture strategy can deliver the right risk-related information. This enables the company to efficiently respond to new business opportunities and to meet risk and regulatory demands consistently and efficiently rather than reactively. Analytics can also enable scenario analyses of stresses on global positions.

9 Deloitte, Risk Transformation: Aligning risk and the pursuit of shareholder value

How can the Board become actively involved in setting risk appetite and embedding it in the company?

Better Practice Guidance

An effective risk appetite framework enables a clear dialogue and alignment of attitudes to risk taking between the Board, senior executives, divisional managers and ultimately all individuals across a company. Leading practices are emerging across a number of sectors and we believe that there is an opportunity for entities to leverage cross industry learnings in this area.

For example, in the financial services sector, the Boards of APRA regulated institutions must ensure that[10]:

- They define the institution's risk appetite and establish a risk management strategy
- Senior management takes the necessary steps to monitor and manage material risks consistent with the strategic objectives, risk appetite statement and policies approved by the Board
- Policies and processes developed for risk-taking are consistent with the risk management strategy and the established risk appetite
- Appropriate controls are established that are consistent with the risk appetite, risk profile and capital strength, and are understood by, and regularly communicated to all relevant staff.

Over the last two years, various global industry and regulator surveys, roundtables and benchmarking studies and exercises have considered refining and operationalising risk appetite frameworks[11]. Their key findings to successfully embed risk appetite frameworks include:

Active leadership and buy-in from the Board

Companies that successfully embed risk appetite frameworks have a Board that is prepared to lead. These Boards are not primarily led or pacified by intermittent reports or sporadic deep dives, but have a level of understanding that challenges and leads the process of setting and monitoring risk appetite and capital adequacy.

A global Risk Management Survey published by Deloitte in August 2013 indicates that 80% of Boards sampled are now actively approving and providing direction on risk policy and risk appetite. These Boards demand more information and clarity around the risks associated with executive decision making, operational processes, and reporting.

Engagement and approval of enterprise level risk appetite framework

As part of the business planning process, enterprise level risk appetite frameworks from leading financial institutions are formally reviewed and approved by the Board or a dedicated Risk Committee of the Board.

Key components of risk appetite are reviewed, assessed, and discussed by business unit management at least annually, and prior to Board engagement, to ensure alignment with the strategic planning process.

Application of risk appetite in decision making and setting of limits and triggers

When interviewed by regulators, the Board and senior executives can give examples of the decisions which were influenced by risk appetite. Those responsible for business risk can also explain what risk objectives they were supporting when particular risk limits and triggers for their business units were set.

Strategic focus and explicit alignment with business strategy and objectives

The Board should set the company's overall strategic plan, objectives and risk capacity at least annually. The Chief Risk Officer or equivalent should set risk strategy, taking into account the company's risk profile, risk appetite and obligations to stakeholders under both normal and stressed scenarios. Financial and non-financial risks and their implications for business models and strategy should also be established.

10 APRA Prudential Standard CPS 220 Risk Management, January 2015

11 Deloitte, Risk appetite frameworks – How to spot the genuine article, 2014

In doing this, the Board should apply extensive judgement on *where*, *when* and *how* to focus and engage with management while providing robust challenges in the design of optimal and desired risk profiles.

Sound risk culture

As indicated by the Financial Stability Board in its guidance for assessing risk culture[12], a sound risk culture determines a company's ability to successfully execute its agreed strategy within its defined risk appetite.

The main challenge for many companies is taking the step between designing a risk appetite framework and effectively implementing it. A risk appetite framework needs to be embedded both from the 'top down' and 'bottom up'. This takes a significant amount of effort and crucially requires buy-in across the company.

The tone at the top is critical. There needs to be full commitment, including debate and challenge, at the Board level. Accurate information needs to reach the Board and be presented in the most effective manner, at the right time.

In addition aligned compensation was highlighted by a regulator as a particularly important driver of cultural change.

Management should facilitate top down direction from the Board by cascading the risk appetite statements, including their ongoing monitoring and control through communication that is meaningful to everyone.

Workshops are effective followed by subsequent communication to all employees reiterating awareness and embedding the approach in daily decision making.

This is complemented by bottom-up information and insight from the businesses and control functions through calibrating risk appetite limits and triggers, as well as reporting risks and the risk profile versus risk appetite.

Timely measurement and monitoring processes

Leading companies have adopted the following practices around measurement and monitoring of risk appetite:

- Performance against risk appetite is reported regularly to the Board of Directors. It can be across a range of timeframes from monthly to annually, and is usually part of 'integrated risk' reporting. This can involve the use of key risk indicators, forecasts, stress testing and scenario analysis. Impact analysis on business activity and decision making, with associated management responses are also useful in engaging the Board.
- Proactive reporting of any risk appetite or limit breach is based on a defined escalation protocol e.g. 'soft' operating limits for internal discussion versus 'hard' limits for Board notification, with included qualitative analysis, for example, management's response.
- A review of risk appetite metrics is performed at least annually or when triggered by a change in risk profile and can be driven by external environment factors and acquisition activities. The Board may evaluate the impact on business activity and decision making.

12 Financial Stability Board, Guidance on Supervisory Interaction with Financial Institutions on Risk Culture: A Framework for Assessing Risk Culture, 7 April 2014

How can a listed entity provide 'sufficient information on how it is recognising and managing risk' for its investors and help them understand and assess their investment risks?

Better Practice Guidance

Listed entities that strive to achieve and maintain excellence in risk governance are taking steps to provide enhanced disclosures of their risk practices to investors. This trend is not only prevalent in Australia but is also emerging in other jurisdictions and we believe that studies in relation to overseas practices can provide an interesting point of reference for Australian entities.

For example, in the US, the Securities and Exchange Commission (SEC) requires disclosure in proxy statements about the Board's role in recognising and managing risks. A study published in 2013 on Board level risk oversight disclosures[13] in proxy statements issued by S&P 200 companies shows a steady upward trend in risk management related disclosures. Ninety-one percent of companies disclosed that the full Board is responsible for risk and at the management level risk-related disclosures increased. A high percentage of companies established a management-level risk committee. The levels of disclosure vary by industry with the financial services sector having the most disclosures given the highly regulated nature of the sector and significant regulatory attention.

13 Deloitte, Risk Intelligent Proxy Disclosures, 2013

Table 1: Trend analysis (132 recurring companies)[14]

Proxy Trending			
	2013	2011	2010
Does the disclosure note that the full board is responsible for risk?	89% | YES	87% | YES	86% | YES
Is the audit committee noted as the primary committee responsible for risk?	66% | YES	63% | YES	64% | YES
Are other board committees noted as being involved in risk oversight	90% | YES	87% | YES	82% | YES
Is the compensation committee disclosed as being responsible for overseeings risk in the compensation plans?	67% | YES	60% | YES	53% | YES
Does the company have a separate board risk committee?	7% | YES	7% | YES	5% | YES
Does the company disclose whether risk oversight/management are aligned with the company's strategy?	45% | YES	45% | YES	39% | YES
Does the disclosure note whether the chief executive officer (CEO) is responsible for risk management or how the CEO is inovolved?	36% | YES	33% | YES	28% | YES
Does the company have a chief risk officer?	22% | YES	20% | YES	18% | YES
Does the company have a risk management committee (at the management level)?	24% | YES	21% | YES	20% | YES
Does the disclosure note how the board is involved with regard to the comapny's risk appetite?	12% | YES	11% | YES	8% | YES
Does the disclosure note the board's oversight with regard to corporate culture?	6% | YES	7% | YES	5% | YES
Does the disclosure separately address reputational risk?	33% | YES	28% | YES	24% | YES

Increased
Constant
Decreased

Source: Deloitte

Board risk-related responsibilities

Around nine in ten companies disclosed that the full Board is responsible for risk (consideration 1) and that the other board committees (other than the Audit Committee) are involved in risk oversight (consideration 3). More than 60% disclosed that the Audit Committee is primarily responsible for risk (consideration 2) and that the Compensation Committee is responsible for overseeing risk in the compensation plans (consideration 4). However, only 7% reported having a board level Risk Committee with the majority of these companies being in the financial services industry.

Management's risk-related responsibilities

The Risk Intelligent Proxy Disclosures study revealed a generally lower percentage of company disclosure in relation to Management risk related practices than of the Board's risk-related responsibilities.

However, almost half those surveyed disclosed whether risk oversight/management is aligned with the company's strategy (consideration 6) and about a third disclosed the CEO's responsibility for, or involvement in, risk management (consideration 7). About a quarter disclosed having a management Risk Committee (consideration 9), although this is now an increasing trend in formalising the risk management infrastructure.

Leading practices

Only 12% of companies disclosed their Board's involvement in risk appetite (consideration 10), which can be difficult to define, particularly in non-financial services companies, and only 6% noted the Board's oversight regarding corporate culture (consideration 11). Yet one-third disclosed separately addressing reputational risk (consideration 12), reflecting a growing concern among S&P 200 companies.

14 Of the S&P companies whose proxy statement were reviewed in 2013, 2011, and 2010, there were 132 companies common to the sample in each year. The trending data shown above is specific to the 2011 and 2013 data

Recommendation 7.1

The Board of a listed entity should have a committee or committees to oversee risk and related disclosure requirements

How can a Board determine if they should or should not establish a risk committee to oversee the entity's risk management framework?

Better Practice Guidance

Does risk oversight warrant a separate Board-level committee? Each Board must answer that question in light of its own needs.

To address increasing risk-related responsibilities, and often to respond to regulatory changes, many Boards have established Board-level risk committees. These include dedicated, stand-alone risk committees, as well as combined hybrid committees (such as an audit and risk committee or asset management and risk committee). Notwithstanding this trend, the full Board remains responsible for risk and risk oversight but a risk committee of either type can further formalise the means and mechanisms by which a Board carries out its risk-related responsibilities.

Key questions to reflect upon when considering the establishment of a Board risk committee are:

What are the natures of the risks the entity will face?
Some entities operate in sectors or industries which require them to manage risks that are well known and understood by the entity and mature over a relatively short period of time. Whilst other entities are faced with new and emerging risks due to the underlying nature of their businesses and the sectors in which they operate. Companies which face, new and emerging risks or 'long tail' risks, that is to say, risks that take a number of years to mature or impact a company's performance would typically require a more structured approach to risk governance.

What are the needs of stakeholders?
The needs of the enterprise and its stakeholders should be considered. It may also suit the Board to assess the quality of the current risk governance and oversight structure, the risk environment, and the future needs of the company. The composition and activities of the risk committee and its relationship with other Board committees could reflect the Board's assessment of those factors.

What is the alignment of risk governance with strategy?
The Board should consider how risk governance is aligned with management's overall strategy. Enterprises vary widely in their business models, risk appetite, and approaches to risk management. A key consideration is how well the Board, management, and business units are aligned in their attitude to risk taking in the context of achieving the strategy intent of the business.

What skills are required to enable the Board or a subcommittee to provide effective oversight of risk?
An entity should consider the skills required to provide effective oversight of the risks faced by the organisation and ensure that Board and committee members' have the required level of skills and experience to discharge their responsibilities.

This is particularly relevant when a Board delegates risk management oversight responsibilities to an combined Audit and Risk Management committee as these traditionally are made up of members with strong financial and statutory reporting skills who may not have a strong understanding of other risks, such as operational risks faced by the organisation.

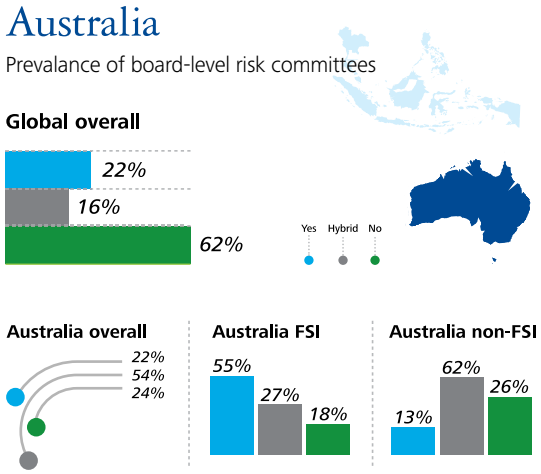
Will the introduction of Board risk committee increase the complexity of risk governance or make it more effective?
Have the current Board and committees been effective in managing risks? Is the enterprise exposed to more unusual risks than others? Does the full Board have enough time to deliberate on risks? Will a dedicated Board risk committee help improve effectiveness and embed an enquiring risk-management culture within the Board?

Given the potential role conflicts and unclear terms of reference among various Board committees, a dedicated risk committee might create unnecessary complexity in the risk-governance structure.

Whatever form it takes, the principle is to keep the risk governance structure simple but effective, avoiding unnecessary complexity for the company.

According to a recent global study[15], Board-level risk committees are well-established and widespread, with 38% of the 400 companies examined globally having either a stand-alone or hybrid risk committee. As might be expected, Board-level risk committees were most often found in financial services industry (FSI) companies, but were also present in other industries — often to a significant extent, depending on the country.

In the same study, the top 50 companies (by market capitalisation as of August 5, 2013) listed on the ASX were analysed in August and September 2013 through a review of company annual reports and committee charters. The analysis shows that 55% of FSI companies in Australia had a stand-alone risk committee while 27% had a hybrid risk committee (82% overall). By contrast, only 13% of non-FSI companies in Australia had a stand-alone risk committee while 62% had a hybrid risk committee (75%) overall.



By whatever means they choose, Boards must fulfil their risk-related roles and responsibilities as effectively as possible. Audit committees, which have traditionally overseen risk in many major companies, face increasing responsibilities for reporting, compliance, and controls. Given these developments, many Boards have established Board-level risk committees.

15 Deloitte, As risks rise, boards respond, a global view of risk committees, 2014

Board workloads have increased, as have those of Audit Committees, which are often tasked with risk oversight. In addition, potential for Board member liability or exposure to legal action for risk-related events or impacts may exist in some jurisdictions.

Given these responsibilities and realities, many Boards have established, or are considering establishing, a risk committee.

Depending on the company, its industry, its risks and its regulatory and risk governance needs, a Board-level risk committee may enable the Board to:

- Assert and articulate its risk-related roles and responsibilities more clearly and forcefully
- Establish its oversight of strategic risks, as well as the scope of its oversight of operational, financial, compliance, sustainability and other risks
- Task specific Board members, and other individuals with overseeing risk and interacting with management and the chief risk officer or its equivalent
- Recruit Board members with greater risk-related experience and expertise
- Be more fully informed regarding risks, risk exposures and the risk management infrastructure
- Improve advice for management on risk, response plans and major decisions, such as mergers, acquisitions, entry into new markets or new lines of business
- Establish clear delineation of oversight responsibilities that support appropriate allocation of resources to both audit and risk management issues.

A Board-level risk committee requires resources, including funding, expertise and time to fulfil its responsibilities which are very similar to those of the Board itself.

Nevertheless given that business, economic, and regulatory environment demands are increasing, as are the magnitude of risks, it is expected that more rather than fewer companies will need to establish a Board-level Risk Committee. The level of formality and rigour that a Board-level risk committee brings to risk oversight responsibilities and risk governance infrastructure is attractive to complex companies.

What is the role of a Board Risk Committee and what should be considered when developing it charter?

Better Practice Guidance

When establishing a Board Risk Committee consider:

- Its role and charter
- How it will provide oversight and required expertise
- Ongoing education of the Board
- Best way to gain visibility into risk management.

Specific roles and responsibilities of the Board Risk Committee are identified in its charter and include the intended means of fulfilling them. The Board Risk Committee should have substantial authority and freedom to craft its charter as it sees fit, and the charter should confer all necessary powers to perform its role. This will usually include the right to obtain information, interview management and internal and external auditors (with or without management present), and seek advice from external consultants or specialists where the committee considers that necessary or appropriate.[16]

Furthermore, the ASX Corporate Governance Council outlines that typically the Board Risk Committee will oversee[17]:

- The adequacy of the entity's processes and practices for managing risk
- Any incident involving fraud or other break down of the entity's internal controls
- The entity's insurance program, having regard to the entity's business and the insurable risks associated with its business.

Other activities may include helping to set and monitor the company's risk appetite, disclosing risk exposures and influencing risk culture.

Other considerations include:

Oversee the risk management infrastructure: A question to consider is whether the risk committee is responsible for overseeing the risk management infrastructure – the people, processes, and resources of the risk management program – or whether another committee or the entire Board will oversee it.
A related issue is whether the Chief Risk Officer or the equivalent will report to the risk committee, the Board, or the CEO – or have a dual reporting relationship to the risk committee, or Board, and the CEO.

Scope of risk committee responsibilities: The Board may need to decide whether the Risk Committee will be responsible for overseeing all risks, or whether other committees, such as the Audit Committee or the Compensation Committee, will be responsible for overseeing some delegated risks.

For example, oversight of risks associated with financial reporting may remain with the Audit Committee, while those associated with executive compensation plans might remain with the Remuneration Committee. But because functional risks (such as tax or human resources risk) are often connected to operational or strategic risks, it is important to consider how the interconnectivity of risks is addressed. In any event, the Board will need to determine which committees will oversee which risks, and redefine the roles of some of the existing committees.

16 Recommendation 7.2 commentary, ASX Corporate Governance Principles and Recommendations 3rd edition

17 Recommendation 7.2 commentary, ASX Corporate Governance Principles and Recommendations 3rd edition

18 Financial Stability Board, Thematic review on risk governance, 2013

Communication among committees: The Board should consider how committees will keep one another – and the Board itself – informed about risks and risk oversight practices. Efficiency and effectiveness call for clear boundaries, communication channels, and handoff points. This need may require the Board to define these elements clearly, making adjustments as needed. The importance of establishing clear communication procedures between the Risk Committee and the Board, as well as across other Board committees, most importantly the Audit Committee, is highlighted in a recent report from the FSB[18].

A part of the commentary in Recommendation 7.1 also states that "A risk committee should be of sufficient size and independence, and its members between them should have the necessary technical knowledge and a sufficient understanding of the industry in which the entity operates, to be able to discharge the committee's mandate effectively."

The company should consider these factors when establishing a risk management committee and thought should be given to how it is addressed when recruiting and selecting directors, particularly if there is a nomination committee. When appointing directors to the risk committee and within the charter of the committee consider whether it is sufficient to have one director with deep industry knowledge and one director with deep technical knowledge? Is a director with risk management expertise required?

Various guides are available including the 'Risk Committee Resource Guide for Boards'[19] which is designed to help companies develop and strengthen their risk committees, and improve risk governance and oversight in the absence of a formal Risk Committee. This Guide includes tools and resources on forming a Risk Committee, a Risk Committee's charter, its composition, responsibilities, education and evaluation.

19 Deloitte, The Risk Committee Resource Guide for Boards. July 2012

Recommendation 7.2

The Board or a committee of the Board should review the entity's risk management framework at least annually to satisfy itself that it continues to be sound and related disclosure requirements

How should Boards review and assess their risk management framework to ensure it is sound?

Better Practice Guidance

It is the role of the Board or the Board Risk Committee to ensure that there is an agreed approach as to how that review will be conducted, who shall conduct it, and how and when to report it to the Board or the Board Risk Committee. This should be done on an annual basis.

There is no commonly accepted practice for reviewing and assessing a risk management framework to ensure that is sound. There is guidance from various sources on suitable approaches and considerations. These include industry bodies such as the Institute of Internal Auditors (IIA)[20], the Financial Stability Board[21], COSO[22], and ISO[23]. Regulators such as APRA[24] also require its regulated entities to undergo an annual review of the risk management framework.

Implicit within all these approaches is that a review of a risk framework addresses the framework itself, its implementation and soundness.

The ISO 31000:2009 'Risk Management Principles and Guidelines' provides advice that a review of the risk framework should:

- Measure risk management performance against indicators, which are periodically reviewed for appropriateness
- Periodically measure progress against, and deviation from, the risk management plan
- Periodically review whether the risk management framework, policy and plan are still appropriate, given the companies' external and internal context
- Report on risk, progress with the risk management plan and how well the risk management policy is being followed
- Review the effectiveness of the risk management framework.

General approaches

The IIA published a guide in 2010 which provides 'three self-contained approaches to assessing the adequacy of risk management based on ISO 31000', which can be summarised as follows:

A process elements approach which determines whether the seven elements of risk management identified in ISO 31000 are in place. The elements include communication, context setting, risk identification, risk analysis, risk evaluation, risk treatment, and monitoring and review.

A key principles approach which states that to be effective a risk management process must satisfy a minimum set of principles or characteristics. ISO 31000 for example has 11 principles.

20 IPPF Practice Guide – Assessing the adequacy of risk management using ISO 31000. IIA 2010

21 Thematic review on risk governance Financial Stability Board. 2013

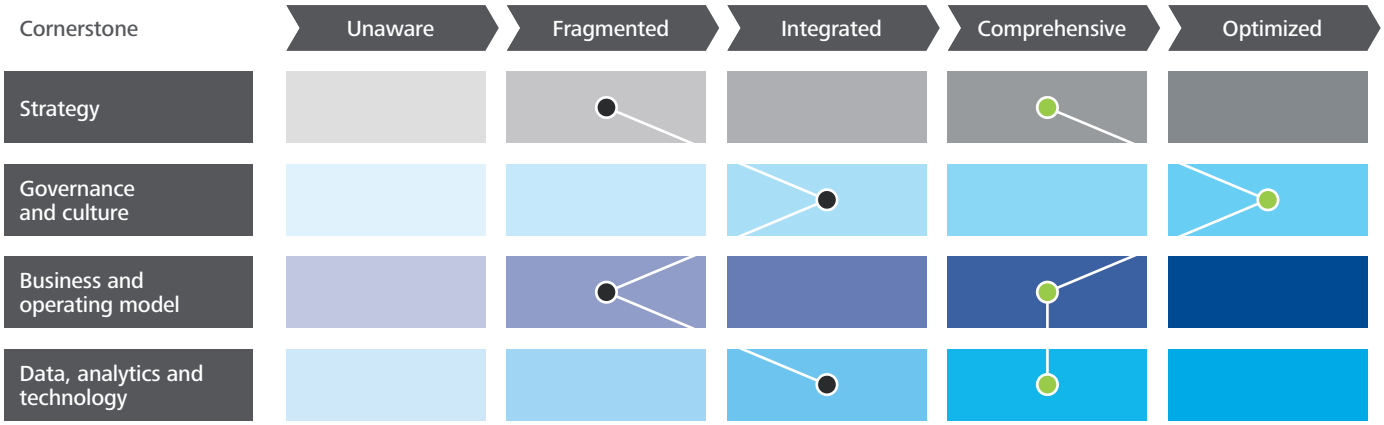
22 Internal Control – Integrated Framework COSO 2013

23 AS/NZS ISO31000:2009 Risk Management principles and guidelines

24 Australian Prudential Regulatory Authority, CPS 220 (Risk Management)

The maturity model approach focuses on improving a company's risk management practices. By putting this approach into practice, a company can understand "where their company's risk management process lies on this continuum" and will subsequently inform the Board whether "it meets the current needs of the company" and meets its maturity expectation.

The maturity model for risk management[25] figure below illustrates how a Board can define maturity of each of the cornerstones of effective risk management across a continuum consisting of five distinct levels of maturity. This approach will assist the Board to determine whether the risk framework meets the current needs of the company.



Source: Deloitte

Boards can ask the following questions about each cornerstone to assess their current state of risk maturity

Strategy

- How clear are our business and risk strategies to internal and external stakeholders?
- How can we improve that clarity?
- How can we bring our risk strategy more in line with our business strategy to support one another?
- How can we allocate capital more efficiently while managing the risks to which the strategy is exposed?

Governance and culture

- Do our governance systems and culture support implementation of our strategy?
- To the extent that we see misalignment, what is the cause?
- What values are – and are not – expressed in our culture?
- How can we drive positive values throughout our culture?

Business and operating models

- How can we best drive awareness and accountability around risk throughout the company?
- How can we achieve regulatory compliance without disruption to our operations?
- Is it possible for a unit to engage in risky activity without the Board's and management's knowledge?

Data, analytics and technology

- How can we leverage our investments in risk management, internal controls and data management and analysis?
- How well do our data management and analytical capabilities support our risk management and regulatory reporting efforts?
- How can we develop an integrated data storage and aggregation infrastructure to support financial, operational, regulatory and risk reporting?

25 *Deloitte, Risk Transformation: Aligning risk and the pursuit of shareholder value*

Recommendation 7.3

A listed entity should disclose: (a) if it has an internal audit function, how the function is structured and what role it performs; and (b) if it does not have an internal audit function, that fact and processes used to evaluate and continuously improve its risk management and internal control processes

What is the right role and structure for internal audit in recognising and managing risk and how is this linked to risk management?

Better Practice Guidance

Internal auditing is an independent, objective assurance and consulting activity. Its core role with regard to enterprise risk management is to provide objective assurance in a systematic, disciplined manner to the Board on the adequacy and effectiveness of the risk management and internal control frameworks.

The specific responsibilities[26] of internal audit include evaluating whether:

- The risk management process has been applied appropriately and that elements of the process are suitable and sufficient
- The risk management process is keeping up with the strategic needs and intent of the company
- Processes and systems are in place to ensure that all material risks have been identified and are being treated
- All prioritised intolerable risks have cost effective treatment plans in place
- Controls are being correctly designed in keeping with the outputs of the risk management process
- Key controls are adequate and effective
- Risks are not over-controlled or inefficiently controlled
- Line management review and other non-audit assurance activities are effective at maintaining and improving controls
- Risk treatment plans are being executed
- There is appropriate and as-reported progress in the risk management plan.

If a listed entity has an internal audit function, the Head of Internal Audit ideally should have a direct reporting line and unfettered access to the Board and to the Board Audit Committee. This is a mandatory requirement for companies which are regulated by APRA[27] and part of the sound risk governance practices suggested by the Financial Stability Board[28].

It is critical for an entity to have a clear understanding of how internal audit relates to, and interacts with, other risk or assurance related functions, such as risk management, legal, compliance, security, health and safety.

This may involve evaluating who is doing what and whether there are any gaps or duplications between internal audit or those groups regarding the assurance being provided.

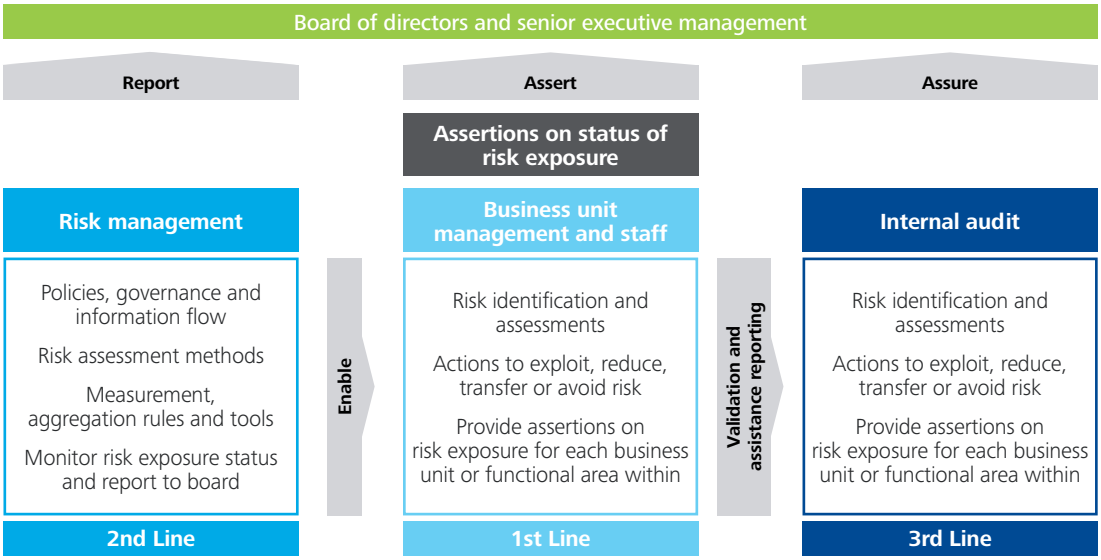
26 The Institute of Internal Auditors, IPPF Practice Guide: Coordinating Risk Management and Assurance, March 2012

27 APRA Prudential Standard CPS 510 (Governance) January 2015, paragraph 90

28 Financial Stability Board, Thematic Review on Risk Governance, February 2013

The **three lines of defence model** is a generally accepted framework used to govern risk and associated risk management and assurance activities in large-scale complex companies.

The first line of defence is typically defined as the line of business where day to day management and risk controls occurs. The second line of defence is Risk and Compliance where risk policies, methodologies and oversight occur. The third line of defence is internal audit where independent assurance occurs. The interactions between three lines are shown below:



When effectively applied, the model enables companies to clearly articulate roles, responsibilities, and associated accountabilities for risk taking, risk management and risk assurance. This model can be used to assist stakeholders understand how the scope and focus of internal audit and risk management functions interact and support risk taking activities in the business.

This concept can be applied to:

- **Clarify roles and responsibilities** for risk identification, management, and assurance across the enterprise for all risk categories
- **Refine the mandate** of the risk management and the internal audit function in light of the risk governance model, determine the target operating model, and associated competencies and skill sets required
- **Leverage to develop a clear transformation plan** outlining how the enterprise can continue to evolve in changing business times.

In structuring the internal audit function, management should consider:

- The activities which will be performed by Internal Audit
- The resources and skills required to provide effective assurance regarding the effectiveness of key controls.

The following questions are designed to assist Audit Committees in their evaluation of their Internal Audit function and the Head of Internal Audit.[29]

1. Does Internal Audit have a clearly articulated strategy that is reviewed periodically and approved by the audit committee?
2. Does Internal Audit have a clear set of performance expectations that are aligned with the success measures of the audit committee, and that are measured and reported to the audit committee?
3. Is Internal Audit appropriately funded or staffed? Is Internal Audit staffed with the appropriate mix of professionals to achieve its objectives?
4. Does Internal Audit have a charter that is periodically reviewed and approved by the audit committee?
5. Does Internal Audit operate in accordance with its charter?
6. Is Internal Audit sufficiently independent of management?
7. Does Internal Audit organise or perform peer reviews or self-assessments of its performance and report the results to the Audit Committee?
8. Is the level of assurance provided by Internal Audit and interaction with other assurance sources clear and appropriate for the audit committee?
9. Does Internal Audit meet regularly with the external auditors to discuss risk assessments, scope of procedures, or opportunities to achieve greater efficiencies and effectiveness across the company's audit services?
10. Is the Internal Audit plan aligned to the key risk of the company and other assurance activities? Is Internal Audit's risk assessment process appropriately linked to the company's Enterprise Risk Management activities?
11. Are issues identified and reported by Internal Audit appropriately highlighted to the audit committee, and is their progress to effective completed management actions tracked and reported?
12. In delivering the annual internal audit plan, is Internal Audit flexible and dynamic in promptly addressing new risks and the needs of the audit committee?
13. Is the work of Internal Audit timely and proactive in the conduct and reporting of issues and addressing them with management?
14. Are reports and other communications from Internal Audit to the audit committee of an appropriate standard of presentation and value provided?
15. Is the Head of Internal Audit respected as an advisor to the audit committee and management on emerging risks of the company?
16. Is Internal Audit highly regarded and respected within the company?

It should be noted that Principle 7.3 (b) provides entities with an option to not have an internal audit function.

29 Deloitte, Key questions for audit committees to ask about Internal Audit, June 2013

Recommendation 7.4

A listed entity should disclose whether it has any material exposure to economic, environmental and social sustainability risks and, if it does, how it manages or intends to manage those risks.

How can a listed entity assess the material sustainability risk exposures and determine if the assessment process is captured effectively within the existing risk management framework?

Better Practice Guidance

This recommendation responds to increasing attention being given by investors and the broader community to econonmic, environmental and social issues and the risks they pose to a listed entity's ability to create or preserve value. This also reflects the increasing importance of both financial and non-financial information to stakeholder decision making in Australia and globally[30].

In this context[31]:

- **'Material exposure'** means a real possibility that the risk in question could substantively impact the listed entity's ability to create or preserve value for security holders over the short, medium or long term
- **'Economic sustainability'** is the ability of a listed entity to continue operating at a particular level of economic production over the long term
- **'Environmental sustainability'** is the ability of a listed entity to continue operating in a manner that does not compromise the health of the ecosystems in which it operates over the long term
- **'Social sustainability'** is the ability of a listed entity to continue operating in a manner that meets accepted social norms and needs over the long term.

Complying with this recommendation may, depending on the nature of the company's activities, include consideration of the following.

Increasing global focus on sustainability reporting and disclosure

Around the world sustainability disclosures are increasing – driven by government regulations as well as voluntary guidelines and frameworks including:

- Integrated Reporting Framework (Global)
- GRI G4 Sustainability Reporting Guidelines (Global)
- Directive on non-financial reporting (EU)
- Grenelle II large company ESG disclosures (France)
- Johannesburg Stock Exchange integrated reporting (SA)
- Conflict Minerals disclosure (USA)
- London Stock Exchange GHG emissions reporting (UK)
- Top 100 listed companies ESG reporting and invest at least 2% of net profits on socially responsible projects (India).

The impact of these global drivers will put more pressure on Australian listed entities to disclose high-quality sustainability information regularly to stakeholders, particularly as Australian entities look to world markets for capital.

30 Principles of Responsible Investment – ascribed to by managers with $34+ trillion FUM (approximately 15% of total global investable assets); ACSI and FSC, ESG Reporting Guide for Australian Companies: Building the foundation for meaningful reporting (June 2011); UN Global Compact's ten principles on human rights, labour, the environment and anti-corruption; OECD's Guidelines for Multinational Enterprises and the Global Reporting Initiative International Integrated Reporting Council

31 Footnote 38 and Glossary, ASX Corporate Governance Principles and Recommendations 3rd edition

Recognising the importance of non-financial information and risks

Recommendation 7.4 elevates sustainability risks and disclosures and is consistent with international trends. This includes various sustainability information reporting requirements adopted by a number of bodies such as the Directive on non-financial reporting adopted by the EU Parliament[32] and others, as well as the release of the Integrated Reporting Framework by the International Integrated Reporting Council (IIRC).

Disclosure of non-financial information is increasingly important with stakeholders as they recognise the need for information on economic, environmental and social impacts to be publicly available and transparent. This is done in order for a company to make good decisions about allocating capital, assessing risks and opportunities to create value and for stakeholders to make investment decisions.

The inclusion of sustainability risks within the ASX Corporate Governance Council Principles means that CFOs, Boards and Audit Committees should specifically consider sustainability issues and risks as they review their corporate governance obligations.

What does this mean for listed entities?

In order to comply with Recommendation 7.4 listed entities should perform an analysis of their exposure to economic, environmental and social sustainability risks and determine their approach to reporting and disclosure. This should be subject to a formal review of the process and outcomes, and also linked to the both business strategy and risk management processes.

The Environmental, Social and Governance (ESG) Reporting guide published by Financial Services Council and the Australian Council of Superannuation Investors[33] suggests the following areas for consideration when **identifying the risks and assess the materiality** for environmental and social sustainability.

Environment

- Climate change
- Environmental management systems and compliance
- Efficiency (waste, water, energy)
- Other environmental issues (for example, toxic and biodiversity).

Social

- Workplace Health and Safety
- Human capital management
- Corporate conduct (for example, bribery and corruption)
- Stakeholder management/license to operate.

Where entities currently report sustainability information this process should be reviewed to confirm that it aligns with the sustainability risk requirements of Recommendation 7.4.

Entities should also consider obtaining independent assurance over sustainability information where they are not currently doing so, in order to increase the rigour of reported information.

Entities should:

- **Review, assess or assure** the application of the entity's materiality and sustainability risk management frameworks and consider which Board committees oversee the economic, environmental and social sustainability risks
- **Confirm who** within the entity is accountable and responsible for conducting the materiality assessment of economic, environmental and social sustainability risks
- **Consider the strategy** for implementing reporting and disclosure – whether in a stand-alone sustainability report or in the Annual Report
- **Consider assurance** of specific statements, information and claims made in corporate reporting and on websites.

32 http://ec.europa.eu/internal_market/accounting/non-financial_reporting/index_en.htm

33 Financial Services Council and The Australian Council of Superannuation Investors, ESG Reporting Guide for Australian Companies Building the foundation for meaningful reporting

Recommendation 4.2

The Board of a listed entity should, before it approves the entity's financial statements for a financial period, receive from its CEO and CFO a declaration that, in their opinion, the financial records of the entity have been properly maintained and that the financial statements comply with the appropriate accounting standards and give a true and fair view of the financial position and performance of the entity, and that the opinion has been formed on the basis of a sound system of risk management and internal control which is operating effectively.

How should the CEO and CFO declaration be worded and what assurance should they obtain before completing the declaration?

Better Practice Guidance

A suggested basic form of sign-off is shown in Appendix B.

As indicated by the ASX Corporate Governance Council in the commentary and other presentations[34], Section 295A of the Corporations Act requires the CEO and CFO of a listed entity provide a declaration that shows that in their opinion the:

- Financial records of the entity for a financial year have been properly maintained
- Financial statements and the notes for the financial year comply with the accounting standards, and give a true and fair view of the financial position and performance of the entity.
- Entity has a sound system of risk management and internal control which is operating effectively.
  The declaration must be given before the directors approve the financial statements for the any financial period as Recommendation 4.2 applies to all financial statements approved by the Board not just the annual financial statement.

Similar requirements may apply to listed entities established in other jurisdictions under local law.

A reasonable level of assurance should be obtained from internal controls. Testing processes adopted are a matter of professional judgment and will vary from company to company.

34 ASX Corporate Governance Council, Commentary for Recommendation 4.2, Corporate Governance Principles and Recommendations, 3rd edition; Transitioning to the third edition of the Principles and Recommendations

Appendix A

ASX Corporate Governance Council Principles and Recommendations 3rd Edition – Principle 7

A listed entity should establish a sound risk management framework and periodically review the effectiveness of that framework.

Being given sufficient information to understand and assess investment risk is crucial to the ability of investors to make informed investment decisions. Recognising and managing risk is a crucial part of the role of the Board and management.

A failure by a listed entity to recognise or manage risk can adversely impact not only the entity and its security holders but also many other stakeholders, including employees, customers, suppliers, creditors, consumers, taxpayers and the broader community in which the entity operate.

Good risk management practices can not only help to protect established value, they can assist in identifying and capitalising on opportunities to create value.

The Board of a listed entity is responsible for deciding the nature and extent of the risks it is prepared to take to meet its objectives.

To enable the Board to do this, the entity must have an appropriate framework to identify and manage risk on an ongoing basis. It is the role of management to design and implement that framework and to ensure that the entity operates within the risk appetite set by the Board. It is the role of the Board to set the risk appetite for the entity, to oversee its risk management framework and to satisfy itself that the framework is sound.

Recommendation 7.1

The Board of a listed entity should:

a. Have a committee or committees to oversee risk, each of which:
   - Has at least three members, a majority of whom are independent director
   - Is chaired by an independent director.

b. And discloses the:
   - Character of the committee
   - Members of the committee
   - The number of times the committee met throughout the period and the individual attendances of the members at those meetings
   - If it does not have a risk committee or committees that satisfy (a) above, disclose, that fact and the processes it employs for overseeing the entity's risk management framework.

Commentary

While ultimate responsibility for a listed entity's risk management framework rests with the full Board, having a risk committee (be it a stand-alone risk committee, a combined audit and risk committee or a combination of Board committees addressing different elements of risk) can be an efficient and effective mechanism to bring the transparency, focus and independent judgement needed to oversee the entity's risk management framework.

The role of a risk committee is usually to review and make recommendations to the Board in relation to:

- The adequacy of the entity's processes for managing risk
- Any incident involving fraud or other break down of the entity's internal controls
- The entity's insurance program, having regard to the entity's business and the insurable risks associated with its business.

A risk committee should have a charter that clearly sets out its role and confers on it all necessary powers to perform that role. This will usually include the right to obtain information, interview management and internal and external auditors (with or without management present), and seek advice from external consultants or specialists where the committee considers that necessary or appropriate.

A risk committee should be of sufficient size and independence, and its members between them should have the necessary technical knowledge and a sufficient understanding of the industry in which the entity operates, to be able to discharge the committee's mandate effectively.

The Boards of some listed entities may decide that they are able to oversee the entity's risk management framework efficiently and effectively without establishing a risk committee. If they do, the entity should disclose in its annual report or on its website the fact that it does not have a risk committee and explain the processes it employs for overseeing the entity's risk management framework.

It should be noted that a listed entity established in Australia is required under the Corporations Act to include in the operating and financial review in its directors' report, a discussion of the main internal and external risk sources that could adversely affect the entity's prospects for future financial years. If a significant event occurs, the entity may also have to disclose the occurrence and its impact under the continuous disclosure requirements in the Listing Rules.

Recommendation 7.2

The Board or a committee of the Board should:

a. Review the entity's risk management framework at least annually to satisfy itself that it continues to be sound
b. Disclose, in relation to each reporting period, whether such a review has taken place.

Commentary

It is important that the Board of a listed entity periodically review the entity's risk management framework to satisfy itself that it continues to be sound and that the entity is operating within the risk appetite set by the Board.

The Board may charge an appropriate Board committee (such as the risk committee or the audit committee) with this task. If it does, this should be reflected in the charter of the committee in question.

When disclosing whether a review of the entity's risk management framework has been undertaken, where appropriate, the entity should also disclose any insights it has gained from the review and any changes it has made to its risk management framework as a result.

Recommendation 7.3

A listed entity should disclose:

a. If it has an internal audit function, how the function is structured and what role it performs
b. If it does not have an internal audit function, that fact and the processes it employs for evaluating and continually improving the effectiveness of its risk management and internal control processes.

Commentary

An internal audit function can assist a listed entity to accomplish its objectives by bringing a systematic, disciplined approach to evaluating and continually improving the effectiveness of its risk management and internal control processes.

If a listed entity has an internal audit function, the head of that function ideally should have a direct reporting line to the Board or to the Board audit committee to bring the requisite degree of independence and objectivity to the role.

Recommendation 7.4

A listed entity should disclose whether it has any material exposure to economic, environmental and social sustainability risks and, if it does, how it manages or intends to manage those risks.

Commentary

How a listed entity conducts its business activities impacts directly on a range of stakeholders, including security holders, employees, customers, suppliers, creditors, consumers, governments and the local communities in which it operates. Whether it does so sustainably can impact in the longer term on society and the environment.

Listed entities will be aware of the increasing calls globally for the business community to address matters of economic, environmental and social sustainability and the increasing demand from investors, especially institutional investors, for greater transparency on these matters so that they can properly assess investment risk.

To meet this recommendation does not require a listed entity to publish a sustainability report. However an entity that does publish a sustainability report may meet this recommendation simply by cross-referring to that report.

Appendix B
Illustrative CEO/CFO certification

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

Please note Principle 7 applies to interim financial statements and annual financial statements. S295A of the Corporations Act 2001 only applies to annual financial statements.

Statement to the Board of Directors of [company]

The Chief Executive Officer and Chief Financial Officer state that:

We, the Chief Executive Officer and Chief Financial Officer of [company] state with regard to the financial statements of [company] for the [period] ended [reporting date] that, in our opinion:

- The financial records of the company for the period have been properly maintained in accordance with s286 of the Corporations Act 2001
- The financial statements and notes thereto comply with Australian Accounting Standards
- The financial statements and notes thereto give a true and fair view of the financial position and performance of the company,

and this opinion 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][35] which is operating effectively.

Chief Executive Officer
[Same date as Directors' Declaration]

Chief Financial Officer
[Same date as Directors' Declaration]

35 ASX Corporate Governance Council, Commentary for Recommendation 4.2, Corporate Governance Principles and Recommendations, 3rd edition; Transitioning to the third edition of the Principles and Recommendations

Appendix C

Key Sources of Information and Useful References

ASX Corporate Governance Council
www.asx.com.au/corporategovernance

Deloitte Risk Transformation
http://www.deloitte.com/view/en_AU/au/services/risk/management/transformation/index.htm

Group of 100
www.group100.com.au

Institute of Internal Auditors
www.iia.org.au

COSO Internal Controls and ERM models
www.coso.org

ISO31000:2009 Risk Management
www.standards.org.au

Deloitte, The value killers revisited: A Risk Management Study
http://deloitte.wsj.com/riskandcompliance/files/2014/05/ValueKiller_pov.pdf

Deloitte, Exploring strategic risk
http://www.deloitte.com/view/en_AU/au/services/risk/management/transformation/7905af934cc82410VgnVCM3000003456f70aRCRD.htm

Deloitte, Aligning risk and the pursuit of shareholder value
http://www.deloitte.com/view/en_AU/au/services/risk/management/transformation/d747541808b22410VgnVCM1000003256f70aRCRD.htm

APRA Prudential Standard CPS 220: Risk Management
http://www.apra.gov.au/CrossIndustry/Documents/Final-Prudential-Standard-CPS-220-Risk-Management-(January-2014).pdf

Deloitte, Risk appetite frameworks – How to spot the genuine article
http://www.deloitte.com/view/en_AU/au/services/risk/management/transformation/f72ac30c6f6b2410VgnVCM3000003456f70aRCRD.htm

Financial Stability Board, Guidance on Supervisory Interaction with Financial Institutions on Risk Culture
(A Framework for Assessing Risk Culture), 7 April 2014
http://www.financialstabilityboard.org/publications/140407.htm

Deloitte, Risk Intelligent Proxy Disclosures 2013, Trending upward
http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/us_grc_Risk_Intelligent_Proxy_Disclosures%20_2013_11152013.pdf

Deloitte, As risk rise, Boards respond – A global view of risk committees
https://www.km.deloitteresources.com/sites/live/crossfunctional/_layouts/DTTS.DR.KAMDocumentForms/KAMDisplay.aspx?List=d78f0933-458e-4f0e-8f7e-f2dabe02af94&ID=661586

Financial Stability Board, Thematic Review on Risk Governance, February 2013
http://www.financialstabilityBoard.org/publications/r_130212.pdf

Deloitte, The Risk Committee Resource Guide for Boards, July 2012
http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/IMOs/Governance%20and%20Risk%20Management/us_grm_rgc_010512.pdf

IPPF Practice Guide – Assessing the adequacy of risk management using ISO 31000, 2010
https://na.theiia.org/certification/Public%20Documents/Assessing%20the%20Adequacy%20of%20Risk%20Management.pdf

Internal Control – Integrated Framework COSO 2013
http://www.coso.org/ic.htm

AS/NZS ISO31000:2009 Risk Management principles and guidelines
http://infostore.saiglobal.com/store/details.aspx?ProductID=1378670

The Institute of Internal Auditors, IPPF Practice Guide: Coordinating Risk Management and Assurance, March 2012
https://na.theiia.org/news/Pages/New-IPPF-Practice-Guide-Released-Coordinating-Risk-Management-and-Assurance,-Supporting-Standard-2050-Coordination-.aspx

APRA Prudential Standard CPS 510: Governance
http://www.apra.gov.au/CrossIndustry/Documents/Final-Prudential-Standard-CPS-510-Governance-(January-2014).pdf

Key questions for Audit Committees to Ask About Internal Audit
http://www.deloitte.com/view/en_US/us/Services/audit-enterprise-risk-services/Internal-Audit-Transformation/7c91fbf677a08310VgnVCM3000001c56f00aRCRD.htm

Financial Services Council and The Australian Council of Superannuation Investors, ESG Reporting Guide for Australian Companies Building the foundation for meaningful reporting, March 2014
http://www.asx.com.au/documents/asx-compliance/esg_reporting_guide_mar14.pdf

Notes

Group of 100
Secretariat
Tel: + 61 3 9606 9661
Email: g100@group100.com.au

www.group100.com.au

Deloitte
Peter Matruglio
National Lead Partner, Risk Transformation
225 George Street
Sydney, New South Wales
Australia
Tel: +61 9322 5756
Email: pmatruglio@deloitte.com.au

www.deloitte.com.au

MCBD_Hyd_11/14_50643