Governance Institute of Australia

Risk management for directors: A handbook

April 2016

About Governance Institute of Australia

Governance Institute of Australia is the only independent professional association with a sole focus on whole-of-organisation governance. Our education, support and networking opportunities for directors, company secretaries, governance professionals and risk managers are second to none.

Our postgraduate education in applied corporate governance and risk management is unrivalled in its breadth and depth of coverage. It sets the standard for entry into the profession. Postgraduate education is also the gateway to membership of the Governance Institute of Australia and the Institute of Chartered Secretaries and Administrators (ICSA) — leading international associations for governance practitioners.

Our Certificates in Governance Practice, Governance and Risk Management and Governance for Not-for-Profits provide skills-based governance and risk management training, and a qualification for a wide range of professionals responsible for corporate accountability functions and processes within an organisation.

Our active membership base of more than 7,000 chartered secretaries, governance advisers and risk managers ensures that the Governance Institute is at the cutting edge of knowledge of issues and support of sound practice in the continuous evolution of governance and risk management.

Foreword

Directors have a fiduciary duty to act in the best interests of the company. In order to discharge their duties, directors need to know, and properly assess, the nature and magnitude of risks faced by the entity. An integrated governance and risk management framework is central both to informed decision-making by the board and adapting to changes in the environment in which the organisation operates.

The governance codes in most developed economies include recommendations for the boards of listed entities to take responsibility for the governance of risk and to delegate to senior management the responsibility to establish a sound system of risk management and internal control, and report regularly to the board on the effectiveness of that system.

In Australia also, the Australian Prudential Regulation Authority (APRA) directs boards of regulated institutions to define the institution's risk appetite and establish a risk management strategy; and ensure 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.

Governance codes and regulators, therefore, place risk attitude (or risk appetite), risk tolerance, and the oversight of the maintenance of sound risk management and internal control systems at the centre of corporate governance and the role of the board in steering organisations. They recognise that risk-taking is what organisations do — risk encompasses the opportunities to be realised by the organisation, as well as the hazards to be avoided, with recognition of the uncertainties attached to the opportunities and hazards alike.

To meet their fiduciary duties, directors must share a common vision of risk, as sound risk management enables knowledgeable risk acceptance. Robust and challenging discussion at the board table concerning the most appropriate vision of risk for the organisation informs the framework that the board of directors adopts to support its risk oversight activities.

This handbook deals with the link between the deliberations of boards and their oversight of management and the alignment of risk management practices with strategic objectives throughout the organisation. It is intended to assist boards to integrate their governance and risk management frameworks. This in turn will assist organisations to achieve strategic focus, by providing boards with the information they need and ensuring ongoing ownership of risks by all employees in relation to achieving strategic objectives.

I thank Judith Fox FGIA who has written this handbook and those members who reviewed it and contributed to its development.

Simon Pordage FGIA
President
Governance Institute of Australia

Table of contents

What this handbook covers

This handbook is aimed at assisting those on the governing body of an organisation to:

- gain clarity about the interaction of governance and risk management
- avoid confusion in the responsibilities of those with an oversight role and those with an implementation role
- achieve focus on embedding risk management within the strategic framework.

ISO 31000:2009 *Risk Management—Principles and guidelines* and the related handbook, HB 436:2004 *Risk management guidelines—Companion to AS/NZS ISO 31000:2009* deal with the implementation aspects of a risk management framework, and will assist entities to focus on operational risk management. Governance Institute's publication *Enterprise Risk Management*[1] also provides a framework for approaching the implementation of risk management.

This handbook deals with the link between the deliberations of boards and their oversight of management and the alignment of risk management practices with strategic objectives throughout the organisation.

This guide is not intended to advise directors on how to create an enterprise risk management system or a technical management-led risk process — these are more suited to development by management. It is intended to assist boards to integrate their governance and risk management frameworks. This in turn will assist organisations to achieve strategic focus, by providing boards with the information they need and ensuring ongoing ownership of risks by all employees in relation to achieving strategic objectives.

The questions that conclude each section are included for consideration and to prompt directors' thinking. Directors will need to decide if they are relevant to their circumstances.

1 Governance Institute of Australia, *Enterprise Risk Management*, 1st edition 2009, updated 2015. Updated version available only on Governance Institute's app http://www.governanceinstitute.com.au/knowledge-resources/publications/governance-institute-app/

Risk management is central to the governance framework

Good governance encompasses not only the system by which authority is exercised in organisations and how they are controlled, but also the mechanisms by which organisations and those who exercise authority within them are held to account.[2]

Those exercising authority and making decisions within an organisation exercise power to facilitate the strategic objectives of the organisation. Each entity is faced with a range of risks that it needs to identify and manage in order to achieve strategic objectives. Risk is the effect of uncertainty on objectives.[3] Accordingly, risk management is a critical area of responsibility for the board.

Directors have a fiduciary duty to act in the best interests of the company. In order to discharge their duties, directors need to know, and properly assess, the nature and magnitude of risks faced by the entity.

An integrated governance and risk management framework is central both to informed decision making by the board and adapting to changes in the environment in which the organisation operates.

A model for board oversight of risk management needs to be viewed from two perspectives. The board has oversight of both strategic and operational perspectives, as illustrated in Figure 1.

Figure 1: A model for board oversight of risk management

2 ASX Corporate Governance Council's *Corporate Governance Principles and Recommendations*, 3rd ed, p 3: 'Corporate governance is the framework of rules, relationships, systems and processes within and by which authority is exercised and controlled in corporations. It encompasses the mechanisms by which companies, and those in control, are held to account'. Definition taken from Justice Owen, HIH Royal Commission, *The Failure of HIH Insurance, Volume 1: A Corporate Collapse and Its Lessons*, Commonwealth of Australia, April 2003 — pg xxxiii

3 International Standards Organisation, ISO 31000:2009: *Risk Management — Principles and guidelines*, 2009

Risk management in governance codes and regulator standards

The governance codes in most developed economies include recommendations for the boards of listed entities to take responsibility for the governance of risk and to delegate to senior management the responsibility to establish a sound system of risk management and internal control, and report regularly to the board on the effectiveness of that system.[4]

Table 1: Division of responsibility for risk management

Body	Responsibility
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.
Management	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.

In Australia also, the Australian Prudential Regulation Authority (APRA) directs boards of regulated institutions to define the institution's risk appetite and establish a risk management strategy; and ensure 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.[5]

Governance codes and regulators, therefore, place risk attitude (or risk appetite), risk tolerance, and the oversight of the maintenance of sound risk management and internal control systems at the centre of corporate governance and the role of the board in steering organisations. They recognise that risk-taking is what organisations do — risk encompasses the opportunities to be realised by the organisation, as well as the hazards to be avoided, with recognition of the uncertainties attached to the opportunities and hazards alike.

To meet their fiduciary duties, directors must share a common vision of risk, as sound risk management enables knowledgeable risk acceptance. Robust and challenging discussion at the board table concerning the most appropriate vision of risk for the organisation informs the framework that the board of directors adopts to support its risk oversight activities.

Directors should be aware of their responsibilities and duties as set out in Table 2.

Table 2: Responsibilities and duties of directors in risk management

Legislation, governance code or regulatory standard	Responsibilities and duties of directors
Corporations Act 2001 (Cth)	s 180 (duty to act with reasonable care and diligence) s 181 (duty to act in good faith in the best interests of the company and for a proper purpose) ss 182 and 183 (duty not to improperly use their position or information)

4 ASX Corporate Governance Council, *Corporate Governance Principles and Recommendations*, 3rd ed, 2014; *The UK Corporate Governance Code*, 2014; *King Code of Governance Principles for South Africa*, 2009 (a draft King IV Code was released for public consultation in March 2016); *Singapore Code of Corporate Governance*, 2012; *Hong Kong Corporate Governance Code*, 2012, *Canada — Corporate Governance Codes and Principles*

5 APRA Prudential Standard CPS 220 *Risk Management*, January 2015

Risk management is central to the governance framework

Legislation, governance code or regulatory standard	Responsibilities and duties of directors
The common law also imposes fiduciary duties on directors	The courts have classified these fiduciary duties under four headings: • to act bona fide in the best interests of the company • to exercise powers for a proper purpose • to retain discretion • to avoid conflicts of interest
Work Health and Safety Act (WHS Act) Implemented in seven out of nine jurisdictions (WA and Victoria have declined to be involved in the WHS harmonisation process) • *Occupational Health and Safety Act 2004* (VIC) • *Occupational Health and Safety Act 2004 1984* (WA)	The primary obligation under the WHS Act is placed on persons conducting a business or undertaking (PCBU) to, so far as is reasonably practical, ensure the health and safety of workers
Principle 7 of the ASX Corporate Governance Council's *Corporate Governance Principles and Recommendations*, 3rd ed, 2014 The governance guidelines developed for listed entities are frequently adopted, or adapted for use, in other corporate structures and also in not-for-profit organisations and public sector entities	Recommendations 7.1: The board of a listed entity should have a committee or committees that oversee risk Recommendation 7.2: The board should review the entity's risk management framework at least annually to satisfy itself that it continues to be sound Recommendation 7.3: The board should disclose if it has an internal audit function, how that function is structured and what role it performs Recommendation 7.4: The board 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. The commentary clarifies that the board delegates to senior management responsibility for the operational effectiveness of the management of risk.

Risk management is central to the governance framework

Legislation, governance code or regulatory standard	Responsibilities and duties of directors
APRA Prudential Standard *CPS 220 Risk Management*, January 2015	An APRA-regulated institution must: • have a risk management framework that is appropriate to its size, business mix and complexity • maintain a board-approved risk appetite • maintain a board-approved risk management strategy that describes the key elements of the risk management framework that give effect to its approach to managing risk • have a board-approved business plan that sets out its approach for the implementation of its strategic objectives • maintain adequate resources to ensure compliance with the Prudential Standard, and • notify APRA when it becomes aware of a significant breach of, or material deviation from, the risk management framework, or that the risk management framework does not adequately address a material risk
Australian Securities & Investments Commission (ASIC) *Regulatory Guide 104 Licensing: Meeting the general obligations* (RG 104)	Guidance to AFS licensees about what ASIC expects in relation to their meeting the obligation to have adequate risk management systems
UK Corporate Governance Code, September 2014 Dual-listed entities	The board is responsible for determining the nature and extent of the principal risks it is willing to take in achieving its strategic objectives. The board should maintain sound risk management and internal control systems.
US Securities and Exchange Commission (SEC) proxy disclosures Companies operating in the US	The commentary clarifies that the board delegates to senior management responsibility for the operational effectiveness of the management of risk.
Environmental legislation • *Protection of the Environment Operations Act 1997* (NSW) • *Environment Protection Act 1997* (ACT) • *Environmental Protection Act 1994* (QLD) • *Environmental Management and Pollution Control Act 1994* (TAS) • *Environment Protection Act 1970* (VIC) • *Environmental Protection Act 1986* (WA) • *Environment Protection Act 1993* (SA) • *Waste Management and Pollution Control Act 1998* (NT)	Directors are subject to liability and must remain vigilant that the organisations they govern maintain a high standard of compliance when they undertake activities that have the potential to result in harm to the environment

Risk management is central to the governance framework

Legislation, governance code or regulatory standard	Responsibilities and duties of directors
Industrial laws Anti-discrimination laws Workers' compensation laws Anti-money laundering legislation	Directors are subject to liability and must remain vigilant that the organisations they govern maintain a high standard of compliance
Commonwealth Department of Finance, *Commonwealth Risk Management Policy*, July 2014	Element One — Establishing a risk management policy Element Two — Establishing a risk management framework Element Three — Defining responsibility for managing risk Element Four — Embedding systematic risk management into business processes Element Five — Developing a positive risk culture Element Six — Communicating and consulting about risk Element Seven — Understanding and managing shared risk Element Eight — Maintaining risk management capability Element Nine — Reviewing and continuously improving the management of risk
Public Governance, Performance and Accountability Act 2013 (C'th)	Provides that the accountable authority of a Commonwealth entity must establish and maintain appropriate systems and internal controls for the oversight and management of risk
There are state and territory exepctations in relation to internal audit and audit and risk committees. For example, NSW Treasury, TPP 15-03, *Internal Audit and Risk Management Policy for the NSW Public Sector*, Version 1.0, July 2015 requires each agency head to attest compliance with the Core Requirements in an Attestation Statement published in the agency's annual report, with a copy provided to NSW Treasury on or before 31 October each year. Expectations in each jurisdiction should be understood.	For example, the NSW Policy requires that government departments and statutory bodies in NSW establish and maintain an effective internal audit function and an independent audit and risk committee.

Shareholder and member interest in board oversight of risk management

All listed entities are expected to apply the principles and practices in a governance code in any given jurisdiction or provide an explanation for why they have not done so.[6] Investors look to the disclosures to make decisions about the deployment of their investment, and are increasingly keen to obtain greater clarity about how well boards are overseeing the management of risk within the organisation and the management team's ability to exercise control. Investors see the board's capacity to present a balanced and understandable assessment of the entity's performance and prospects as key to whether a board is adequately undertaking its responsibility to act as the agent of shareholders to preserve and create value on their behalf.

Members in non-listed organisations, while not necessarily seeking to make decisions about the deployment of financial investment, are equally keen to assess the capability of the board to:

- set the risk appetite for the organisation
- oversee the risk management framework implemented by management, and satisfy itself that the framework is sound.

Public sector entities with boards are created to carry out certain functions for government that have been approved by the responsible Parliament and the relevant Minister(s) will have an interest in the accountability of the board in respect of its oversight of risk management within the entity. Integrity and central agencies such as the Auditor-General, the Public Service Commission, the Ombudsman, anticorruption bodies and Departments of Treasury and Finance may also have an interest. Public sector entity boards also need to take account of the interest of other stakeholders, including the community, in the oversight of risk management.

The role of the board

The board is ultimately responsible for deciding the nature and extent of the risks it is prepared to take to meet objectives.

The board needs an appropriate blend of non-executive and executive directors. This includes having a sufficient number of independent non-executive directors who can challenge management and hold them to account and also represent the best interests of the organisation and its members as a whole rather than those of individual members or interest groups.

Board renewal is critical to performance. The board of directors should regularly assess the composition and effectiveness of the board as a whole, as well as any upcoming need for new directors, which will include a review of the required mix of skills, experience and other qualities of directors.[7] A useful tool to assist the board in determining the right mix of directors and understanding its renewal needs is a skills matrix.[8] A skills matrix is crucial to the process of determining director nominations — it functions as a risk management tool for the board. Factors to be taken into account when developing such a matrix should include not just the skills and experience, but also the personal attributes and diversity required of directors, both collectively and individually.[9]

---

6 The Australian Securities Exchange (ASX) Listing Rules require disclosure in annual reports or on websites of the extent to which the corporate governance frameworks and practices of listed entities align with or differ from the principles and recommendations set out in the *Corporate Governance Principles and Recommendations* (the 'if not, why not' regime).

7 ASX Corporate Governance Council, *Corporate Governance Principles and Recommendations*, 3rd edition, 2014, Recommendation 1.6, p 13

8 ASX Corporate Governance Council, *Corporate Governance Principles and Recommendations*, 3rd edition, 2014, Recommendation 2.2, p 15

9 Governance Institute of Australia, *Good Governance Guide: Creating and disclosing a board skills matrix*, http://www.governanceinstitute.com.au/media/762794/ggg_creating_disclosing_board_skills_matrix.pdf

Risk management is central to the governance framework

All directors upon induction and thereafter should understand the entity's business and the material business risks it faces. The chair of the board should regularly review and agree with each director his or her training and development needs to ensure that the directors as a group have and maintain the skills, knowledge and familiarity with the organisation required to fulfil their role on the board and on board committees effectively.[10]

Checklist for directors: Risk as the effect of uncertainty on objectives

- Are there processes in place to integrate risk management into strategic planning?
- Does the overall strategic planning process consider and prioritise the uncertainty attached to achieving strategic objectives across the organisation?
- Does management need to be encouraged to incorporate value creation as well as preservation into its risk management framework?
- Does the board consciously assess risk and reward when considering major strategic initiatives?
- Do the board's agendas promote integration of risk issues with other agenda items such as strategy, organisational structure and finance?
- Does the board assess strategic plans in terms of their potential failure and the attendant consequences?
- Does the board have an adequate framework to understand the interrelationships, interdependencies and compounding effect of risks?
- Does the board analyse the proposed means of reaching those goals, and the likely constraints?
- Does the board act as a catalyst to bridge silos in the business by bringing various risk owners into the same room to present their perspectives and strategies on risk?
- Does the board have a view on who is the designated person with responsibility for risk management within the organisation, the person who will work with the risk owners, each of whom has responsibility for managing different aspects of risk operationally? For example, it could be the company secretary in a smaller organisation or a chief risk officer in a larger organisation.
- Is the board confident that there is communication and understanding between those responsible for reviewing the management of opportunities and the risks attached to them across the organisation and those responsible for articulating organisational messages?
- Does the board appropriately allocate risk management resources?

Board committees

The ultimate responsibility for the oversight of risk management lies with the board. In exercising this responsibility, boards often establish committees with a focus on particular aspects. Two areas of focus are common:

- risk oversight and internal control
- integrity of financial reporting.

These are closely related (inaccurate financial reporting is just one risk among many, and many other risks have financial reporting implications), so often a single committee examines both. Nevertheless, it is also common for organisations to have a separate audit committee in addition to one or more risk committees.

10 ASX Corporate Governance Council, *Corporate Governance Principles and Recommendations*, 3rd edition, 2014, Recommendation 2.5, p 18

Risk management is central to the governance framework

The audit committee is mandated in Australia for the S&P/ASX top 300 companies and is required for many other organisations by various form of regulation. All other listed entities are recommended to establish an audit committee under Principle 4 of the ASX Corporate Governance Council's guidelines. APRA requires the establishment of an audit committee in the entities that it regulates.[11]

The ASX Corporate Governance Council's Principle 7 includes a recommendation that listed entities establish a committee or committees to oversee risk, but does not specify that it has to be a stand-alone risk committee, or combined with audit.[12] While risk committees are not mandated for APRA-regulated entities, the regulator confirms that APRA expects that the board will have considered the necessity of such a committee and the suitability of arrangements for dealing with risk issues at the board level.[13]

Governance codes globally recommend that the board establish an audit committee, where it is not mandated by listing rules. The US has imposed more specific rules through the New York Stock Exchange (NYSE) which requires that audit committees of listed companies discuss the risk assessment and risk management policies of the organisation.

Combined audit and risk committee or stand-alone risk committee?

It has been argued that combining audit and risk on the one committee can lead to a backward-looking focus, given the audit committee responsibility for the oversight of, and reporting to the board on, the financial accounts and adoption of appropriate accounting policies, internal control, compliance and other matters. The argument for a separate risk committee points to the need for the risk focus to be forward-looking, with a consideration of opportunities and uncertainties with respect to those opportunities. These arguments, however, overlook prospective aspects of financial reporting (the emergence of new risks and changes in existing ones) and the need for risk committees to monitor and review the effectiveness of the controls the organisation has put in place.

A risk committee, typically:

- provides oversight of activity and advice to the board in relation to current and potential future risks and risk management strategies (possibly in relation to a specified subject area)
- provides recommendations about risk appetite and tolerance
- monitors the management of risk within its remit
- identifies to the board any matters within its remit where it considers that action or improvement is needed and recommends the steps to be taken.

Many listed entities will have more than one committee responsible for the oversight of different elements of risk, such as workplace health and safety, sustainability, investment and environmental impact. Essential is the manner in which board committees communicate with each other and to the board to ensure that each committee benefits from the insights of the other committees. In some companies it is organised so that any director can attend any committee meeting.

---

11 Australian Prudential Regulation Authority, *Prudential Standard CPS 510 — Governance*, p 14, January 2015

12 ASX Corporate Governance Council, *Corporate Governance Principles and Recommendations*, 3rd ed, 2014, Recommendation 7.1, p 28. The commentary to Recommendation 7.1 notes that: '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 judgment needed to oversee the entity's risk management framework.'

13 Australian Prudential Regulation Authority, *Prudential Practice Guide CPG 220 — Risk management*, January 2015

There is no one model that is suitable for all organisations. For some organisations, combining the oversight of audit and risk may bring clarity, particularly where the major risks are financial ones. For other organisations, separating the focus could bring greater benefit, with the audit committee concentrating on the financial risks and the risk committee or committees concentrating on other significant business risks.

For some organisations, the committee structure is mandated. For example, APRA mandates that an APRA-regulated institution must establish a board audit committee and a board risk committee[14] and NSW Treasury mandates a combined audit and risk committee for all NSW government departments and statutory bodies.

Regardless of the committee structure, there can only be one management process within the organisation and there should be a single, integrated view of risks presented to the board.

Internal audit and external audit

The board needs to satisfy itself that the risk management framework established by management is operating effectively and as intended. It tests the effectiveness from time to time through assurance providers such as internal and external audit.

An internal audit function brings a systematic, disciplined approach to evaluating and continually improving the effectiveness of the organisation's risk management and internal control processes. The head of that function should have a direct reporting line to the board or to the board audit committee (and risk committee or committees if separate) to ensure there is independence of assurance.

Smaller organisations may not have an internal audit function, but should be able to demonstrate the processes in place for evaluating and continually improving the effectiveness of their risk management and internal control processes.

The 'three lines of defence' can be a useful way to define roles and responsibilities when considering effective risk management and control:

- First line — operational management control
- Second line — management assurance (risk control and compliance oversight functions established by management), and
- Third line — independent assurance.

The board and its committee(s) are not included in the 'three lines of defence' but are served by the 'three lines'. Their role is to ensure that the 'three lines of defence' model is reflected in the organisation's risk management and control processes.

14 Australian Prudential Regulation Authority, *Prudential Standard CPS 510 Governance*, January 2015

Risk management is central to the governance framework

Questions directors can ask about risk and board committees

- Do we need separate committees for audit and risk?
- Does every board committee have risk on its agenda?
- Does each board committee report to the full board, so that it can process the information to develop a full-spectrum picture of risk?
- Is risk seen as the responsibility of one committee only?
- Does the board take ownership of risk across the organisation?
- Does the board view itself as the catalyst to bridge the gaps between knowledge among different silos within the organisation?
- Are there reputable experts to advise the board on various risk matters and does the board regularly engage such experts?
- Has the organisation clarified the processes by which the board can seek independent advice?
- Has it defined the role of the company secretary as a dedicated support for non-executive directors on any matter relevant to the business on which they require advice separately from or additional to that available in the normal board process?
- How does the board satisfy itself that the risk management framework established by management is operating effectively?
- Does internal audit have unfettered access to the board?
- Does the board have a Q&A session with internal audit employees once a year?

Culture

What does culture mean?

An organisation's culture is the sum of its shared values and behaviours. It includes the values and behaviours of its people as they relate to various dimensions, such as risk, but those dimensions are not separate cultures.[15] References are commonly made to an organisation's innovation culture, safety culture or compliance culture — these are simply dimensions of the organisation's culture.

Culture is a key determinant in the performance of an organisation and its capability to achieve its objectives. It goes to the heart of the openness and transparency needed for effective stewardship and informed decision-making.[16]

Table 3: Division of responsibility for culture as part of risk management

Responsible body	Responsibility
The board	Define and set the culture of the organisation
Management	Implement the values and behaviours as defined and set by the board as appropriate for the culture of the organisation

The question for boards is whether the culture is known and understood and whether the actual culture (the lived culture) represents the necessary and desired culture. It is an essential element of governance for a board to understand if there is any disjunction between the desired and stated culture and the actual culture, for it is only the actual culture — the enacted values — that ultimately matter.

An organisation may have sub-cultures, which are intra-organisational groups of people who exhibit a set of shared values and behaviours that are identifiably different from those in other areas of the organisation. Boards and management need to identify if there are subcultures within the entity that do not align with the desired culture of the organisation as a whole: any 'rogue' subcultures should be identified.

Rules are necessary but not sufficient to inculcate a culture where the enacted values align with the desired values. Also, without an open and transparent culture, the questioning that will test if the enacted values align with the desired values will not be undertaken. Both go to the heart of governance and risk management if they are to create and protect value for the organisation.

15 A useful working definition is: 'a set of shared mental assumptions that guide interpretation and action in organisations by defining appropriate behaviour for various situations' (Ravasi and Schulz)

16 Opening remarks of the Hon Justice Owen in the *Final Report of The HIH Royal Commission* (2003): 'From time to time as I listened to the evidence about specific transactions or decisions, I found myself asking rhetorically: did anyone stand back and ask themselves the simple question — is this right? … Almost every facet of life is governed by rules, regulations, proclamations, orders, guidance notes, codes of conduct, and so on… There is no doubt that regulation is necessary: peace, order and good government depend on it. But it would be a shame if the prescription of corporate governance models and standards of conduct for corporate officers became the beginning, the middle and the end of the decision-making process… I think all those who participate in the direction and management of public companies, as well as their professional advisers, need to identify and examine what they regard as the basic moral underpinning of their system of values. They must then apply those tenets in the decision-making process.'

Risk-aware culture

The risk culture of an organisation is the shared attitudes (values) and behaviours of individuals about the management of risk in an organisation. The organisation's culture will be a key determinant in its ability to respond and adapt to changes in the environment in which the organisation operates.

To effectively manage risk and leverage the opportunities created by uncertainty, an organisation needs a risk-aware culture. A risk-aware culture is a critical subset of the broader organisational culture that incorporates the way directors, managers and employees think, communicate and behave about all aspects of risk.[17]

Organisations should be alive to cross-cultural differences and their implications. People play the crucial role in defining and sustaining cultural attitudes. As a result, focusing on the particular aspects of people's identity that can have an impact on culture can be an important means of providing insight into understanding why a culture operates as it does. The role of people's national cultural identity is influential in organisational culture. National cultures have different values and therefore different behaviours may be anticipated in response to a common situation. Research has pointed to national differences in the way people tend to deal with uncertainty, and these are important in understanding people's attitudes toward risk.[18]

Risk appetite

Setting the risk appetite explicitly articulates the attitudes to and boundaries of risk that the board expects senior management to take. The board provides a series of licences to senior management to act in particular ways or implement particular decisions that align with these attitudes. Senior management in turn sets in place a further series of licences that cascade the risk appetite through the organisation to align decision making at all levels with the attitudes to risk set by the board.[19]

The concept of risk appetite seems easy to grasp, yet in practice answering the question of the amount and type of risk an organisation is willing to pursue or retain can be very difficult. The risk appetite statement should be descriptive enough to give its audience an understanding of the approach the organisation takes to managing risk and the weighting of risk against potential reward. Risk appetite is strategic and directly related to the achievement of business objectives, including the allocation of resources. The risk appetite statement can be both quantitative and qualitative.

The risk appetite statement may consist of high-level statements in only one or two paragraphs that in turn drive a more detailed listing of risk tolerances. The two parts work together and in their entirety constitute the risk appetite statement.

17 APRA's Prudential Standard (enforceable) for authorised deposit-taking institutions (ADIs), general insurers and life insurers states that the board must ensure that it: 'forms a view of the risk culture in the institution, and the extent to which that culture supports the ability of the institution to operate consistently within its risk appetite, identifies any desirable changes to the risk culture and ensures the institution takes steps to address those changes'.

18 Hofstede's cultural dimensions theory, as articulated in *Culture's Consequences and Cultures and Organizations: Software of the Mind*, co-authored with Gert Jan Hofstede

19 ASIC's report on AFS licence holders indicated that determination of risk appetite is a board responsibility. APRA's Prudential Standards (enforceable) for ADIs, general insurers, life insurers and superannuation require boards to maintain and approve a 'risk appetite statement'. The Committee of Sponsoring Organisations of the Treadway Commission (COSO) proposes that management, with board review and concurrence, should develop risk appetite; communicate risk appetite; and monitor and update risk appetite

Risk appetite statement

The risk appetite statement reflects the board's vision for the organisation. While regulators may prescribe a range of contents for the statement, it is generally accepted that such a statement should reflect the:

- strategy of the organisation — objectives, business plans, stakeholder expectations
- capacity of an organisation to absorb loss — the tolerance for loss or negative events that can be reasonably quantified
- ethical stance of the organisation (activities that are not acceptable and classes of risk to be avoided)
- skills, resources and technology required to manage and monitor exposures
- willingness of the organisation to invest in pursuit of its strategic objectives — multiple risk appetites may exist for different types or sources of risk
- expected return on investment — that is the amount that the organisation is prepared to spend to improve likely outcomes.

Setting appropriate boundaries for risk-taking is the core function of risk appetite and risk tolerance.

Table 4: Difference between risk appetite and risk tolerance

Risk appetite	Risk tolerance
Strategic	Tactical and operational
Part of whole-of-organisation governance	Enables an organisation to control its appetite for risk in line with organisational, strategic objectives
The broad pursuit of risk	The level of risk that can be borne in the context of specific transactions or activities. There will be occasions where an organisation has the propensity to take more risk than it is normally thought judicious to pursue, if there are trade-offs or rewards that justify such behaviour

Questions directors can ask about risk appetite

- Is the risk appetite defined and articulated and can it be understood by its audience?
- Is the risk appetite reviewed on a regular basis?
- Are risk tolerances identified?
- Is risk handled in accordance with the risk appetite and tolerances? What are the areas of risk that have been assessed by management as outside the board's risk appetite? Have they been reported to the board?
- Does the board know what risks management is bringing into the business and whether these are aligned with the risk appetite?
- Have the intolerable risks been identified: those that will put the organisation out of business?
- Are risk management failures seen as learning opportunities?
- Is there an over-reaction to risk management failures, with the risk that there will in future be a reluctance to report failures?

Incentives

Incentives play a powerful role in influencing the values and behaviour of individuals, and hence the culture.

Incentives may have unintended consequences. Research has shown that individuals will seek to do those things that are rewarded, often to the exclusion of activities that are not rewarded. This can create cases of folly, however, where the types of behaviour rewarded are those which the organisation is trying to discourage, while the desired behaviour is not rewarded at all.[20]

Examples include:

- We hope for long-term and sustainable growth — but reward quarterly sales.
- We hope for team work — but reward individual effort.
- We hope for safer workplaces — but reward productivity and cost reduction.
- We hope for candour — but reward reporting of good news and agreeing with the boss and punish reporting of bad news or disagreement with the boss.

The role of the non-executive director with an independent mind

One of the key characteristics that members expect of a well governed organisation is the exercise by its board of independent judgment made in the best interests of the organisation and its members generally.

To successfully develop a culture of openness and transparency, the behaviours of directors need to be commensurate with the stated values of the organisation, and that can only be facilitated by robust and open discussion and debate. Behavioural expectation involves a readiness to test and challenge and, in respect of risk matters, a readiness to seek external advice in doing so if it is felt to be appropriate.

The independence of mind of non-executive directors provides a foundation for inquiry and for building openness with and trust from senior executives. In turn, management needs to recognise the contribution that non-executive directors make to such cultural values.

Challenging specialist knowledge is particularly important, as the willingness to listen to and respond to a contrary opinion is one indicator of an open and transparent culture. The expertise of non-executive directors is therefore an important tool in assisting a board to review the degree to which the culture is one of being open to challenge.

Board evaluation of the lived culture

For a board of directors, it can be very challenging to understand the degree to which the culture reflects the values it espouses. Equally challenging for a board is to put in place the strategies necessary to develop such a culture.

However, boards can turn to various metrics and methods to assist them in this quest. For example, tools are available for boards to gauge stakeholder views of the culture of the company. Surveys of customers and their degree of satisfaction are important, and can be merged with a variety of different analytical tools that provide feedback on the strategic performance of the company. Other tools such as staff engagement and leadership behaviour surveys provide valuable insight, as do reports on the safety culture operating in the organisation.

20 Kerr, S, 'The folly of rewarding A, while hoping for B', *Academy of Management Journal* , Dec 1975; 18, 000004, p 769

Culture

Relying on the history of the business does not provide complete insight into the culture operating within the organisation currently, although it can form part of the information available to the board in forming a view of whether the culture reflects the vision of the board.

A board can organise for expert consultants to provide a briefing to inform the directors of what occurred in a company that did not identify or manage its risks, providing a step-by-step study of the process. This can provide insight into issues of culture that may not have been apparent from the results of other methodologies used.

Questions directors can ask about culture (values)

- Does the board understand what underpins the reputation and ongoing viability of the organisation?
- Does the board have a sense of the culture operating in the organisation?
- Is there a consistency between the actions of employees and the values of the organisation?
- Has the board considered the likely impacts of the incentives in place on behaviours and values?
- Has the board established mechanisms for satisfying itself that a culture that allows, rewards and encourages openness is in place?
- Are issues seen from the perspective of external stakeholders as well as from an internal perspective?

Questions directors can ask in relation to behaviour underpinning the values

- Is the tone around risk set, clearly and consistently, from the top?
- Are the desired behaviours enacted by management?
- Is opportunistic behaviour encouraged?
- Are there accountability mechanisms in place to ensure that the lived values and behaviours of management align with the desired values and behaviours?
- Are there consequences for individuals if they fail to enact the desired values and behaviours?
- Is there defensiveness about organisational culture?
- Do the engagement results of employee surveys identify regular concerns or conflicts of interest or a fear of speaking up?
- Are there regular breaches of regulation?
- Does the style and entrenchment of the CEO block the possibility of constructive challenge from within the executive team?
- Does the CEO exhibit a degree of concern, if not resentment, that challenge from the non-executive directors is unproductively time-consuming, adding little or no value, and potentially intruding on or constraining the ability of the executive team to implement the agreed strategy?
- Does the CEO point to the risk and audit committee(s) or function when risk management is discussed rather than talking of risk management in terms of the business and management?

Questions directors can ask about the incentives

- Are both the overt and implicit incentives aligned with either the stated values of the organisation or the mitigation framework to prevent undue risk-taking?
- Is this monitored constantly?
- Does the board include risk management as a criterion for executive evaluation?
- Are current remuneration practices aligned or at odds with the risk tolerance/capacity of the organisations?
- How much pay is at risk?
- Does fixed remuneration form the larger part of short-term behaviour?
- Is the construction of remuneration systems and targets driven by shareholders with short-term performance targets?
- Are risk-related objectives built into the company's executive remuneration structures?

People

Management's role

It is the role of management to design and implement the risk management framework and to ensure that the organisation operates within the risk appetite set by the board.

Within the risk appetite, framework and process approved by the board, risk has to be managed within the business. It is not managed by the board, the risk committee or the risk management unit, but operationally.

In most large organisations, there will be a person or team responsible for managing risk. The seniority of the head of risk management varies. However, there is rarely a single person or team responsible for coordinating the information on risk across the organisation and synthesising that information for the board. Usually, different teams (for example, finance, operations, public relations, executives) handle different aspects of risk.

Business managers manage risk every day in relation to the products and services they offer or wish to offer, but may have a narrow understanding of how those risks either align with or verge from the organisation's risk appetite or strategy. Conversely, those managers supporting the business units, such as legal, taxation and human resources, may lack an understanding of how their expertise specifically applies to the products and services on offer.

It is the business strategy that unites the efforts of disparate aspects of the business. Yet in many companies, the business strategy may be poorly understood or poorly communicated outside of the executive team or rarely measured throughout the organisations. In order for an understanding of risk to cascade through the organisation, management teams need to understand:

- the priorities of the organisation
- the rationale for funding certain projects and not others, and
- the expected results from that prioritisation, including how those results will be measured (for example, customer satisfaction, market penetration, financial growth).

To embed an awareness of risk in the company it needs to be defined not only as hazards to be avoided, but also as opportunities to be realised and the uncertainties attached to those opportunities. Clarifying this definition throughout the business enables all employees to understand that risk and its management is essential to the growth of the business. In turn, this enables clarity about who is required to take ownership of particular risks within the organisation , with concomitant reporting responsibilities on the management of those risks.

Governance Institute's *Guidelines: whole-of-organisation governance* provide a framework for an organisation to:

- ensure that the effort undertaken by all employees across the organisation is aligned with the strategic objectives

- clarify individuals' roles, authorities and accountabilities in achieving strategic objectives
- empower individuals to make decisions that are aligned with strategic objectives
- clarify the controls and boundaries that apply to the exercise of authority
- provide for clear and effective accountability for the decisions taken and authority exercised.

A clear whole-of-organisation governance framework supports the achievement of the organisation's strategic objectives by clarifying that decision-making is tied to risk and there is accountability for the exercise of authority. Such a framework allows all employees to respond to changing circumstances, while ensuring that decisions are made within the risk appetite set by the board.

Management should establish mechanisms to:

- monitor exposure and risk management performance — monitoring risk appetite at an organisational level means that there needs to be a clear and defined way to escalate risk monitoring results from all the areas of the organisation
- approve the retention of risks
- enforce the risk tolerances prescribed by the board — an effective risk appetite statement will shape the way the organisation is managed
- routinely monitor and evaluate the risk management processes and report to the board.

Appointing the right management team

Good governance demands an appropriate separation between those charged with managing an organisation on a day-to-day basis and those responsible for overseeing its managers.

Effective risk oversight begins with a solid, mutual understanding of the extent and nature of the board's responsibilities as compared to those of management and other stakeholders. The ultimate goal is to assist boards to have confidence in the information they receive from management, and management to create a cohesive process in which risks and their impacts are routinely identified, evaluated, and addressed. The assessment of risk to reputation and organisational viability is the responsibility of both parties.

One of the most important roles of a board is to select, appoint and, if necessary, replace the chief executive officer. In many organisations, the board will also approve the appointment, and when necessary replacement, of other senior executives.

The capacity of directors to bring independent judgment to bear on decision making and challenge of executives is important in preventing domination of a board by any one individual — the CEO being the most likely to fit this role. A culture of immense momentum can build up in a company, in which disagreement with the forward momentum can be difficult. The capacity of non-executive directors to question and challenge management is fundamental to evaluating and managing opportunities and the uncertainties attached to them, and this can be even more necessary at times of apparent business success. Such questioning relies on a clear understanding of the strategic risks and opportunities facing the organisation.

Delegations of authority

Whole-of-organisation governance is about how authority is exercised and controlled below the board in an organisation. Authority cascades from the board to the CEO to the executive management team and throughout the organisation.

- All decision-makers in the organisation should understand the purpose for which authority is to be exercised — to facilitate the strategic objectives of the organisation (the why).
- All decision-makers should understand how authority is exercised, who has authority to do what, and what boundaries apply (the how).
- Appropriate monitoring mechanisms should be in place to provide assurance that decisions are being made in the right way for the right purpose (the safeguard).

The board needs to know that an effective framework is in place clarifying who is authorised to make what decisions and in what circumstances. Comprehensive delegated authorities should be put in place by management, clearly articulating to each decision maker within the organisation their capacity to make decisions in relation to their specific responsibilities and duties. The delegations of authority framework needs to align with the strategic objectives of the organisation.

The delegations policy should clarify that setting out the delegations of authority is a fundamental component of a risk management framework. It is not a stand-alone policy, but central to the governance framework of an organisation both at and below board level. It provides a framework for decision-making and accountability within the organisation.

Governance Institute's *Good Governance Guide: Issues to consider when developing a policy on delegations of authority* is a useful reference.

When framing delegations of authority, management needs to consider them within the risk management framework through scenario testing. This could include considering the risks of unintended consequences if this particular form of empowerment is granted. Management needs to ensure that all material decisions, both financial and non-financial, are covered by the delegations of authority.

Appropriate training

The board needs to be actively involved in the process of identifying and assessing the strategic risks that will be a key input into developing and approving the strategic plan. It is then also useful, following the development of the strategic plan but before it is finally approved, to subject it to a stress test to determine whether it will be able to be implemented within the organisation's risk appetite. That will include determining whether elements of the strategy will have material impacts on the organisation's operational risks that may require either significant work to enable an effective operational control environment or to make adjustments to the strategy.

Training may be essential for all non-executive and executive directors to assist in this process. Training should also extend throughout the organisation (from the top to the coal face). In this way, skills are developed from team leaders to the CEO to the board and back again.

Questions directors can ask about accountability

- Does the board establish and reinforce executive accountability for risk management?
- Does the CEO set and demonstrate consistency in relation to accountability for values and behaviours?
- Does the board expect full disclosure by management of the risks associated with each aspect of the strategy?
- Does the board provide management with ongoing feedback about its satisfaction with their level of disclosure and the quality of risk-reward analyses?
- Are risk management accountabilities built into job descriptions, training, work processes, supervisory procedures, and performance appraisals?
- How is risk management linked with individual employee performance?
- Is the delegations of authority framework consistent with the risk management framework?

Structures

Risk management function

The risk management function needs to be sufficiently close to the business to properly advise the business and at the same time sufficiently separate from the business to fulfil its assurance function. Balance between these two aspects of its function is necessary. The organisation needs to decide for itself the balance. In large organisations these functions may be separate roles and held by different individuals, but this may not be the case in smaller organisations.

It can be useful to have a dedicated risk management function, but this will depend on the size of the organisation. By coordinating the participation of all aspects of the business in risk management, a risk management function relies on information that is already available. It also develops channels of communication to ensure that strategy and risk appetite are central to developing risk management strategies and that information from a variety of sources across the business is synthesised for reporting to the board.

If the organisation has a risk management function, and seeks to implement an enterprise risk management framework, it needs to be structured and have a mandate to fulfil its role and accountabilities.

It is important that a separate risk management function not become trapped in a silo separate from the operational business units. However, it is also important that the risk management function not be 'captured' by the business functions. The risk management function must work closely with and be supportive of the businesses but at the same time retain sufficient independence to question their decisions and, if necessary, escalate their concerns.

A shared language concerning risk management also unites the various disciplines in a common effort to achieve organisational goals. The organisation needs a unified view of risk across all business units.

APRA-regulated entities are required to have a designated risk management function and must designate a chief risk officer to be responsible for that function.[21] Where a chief risk officer or risk management function operates in entities that are not regulated by APRA, the board should ensure that they have an independent line of reporting to the board.

The size, business mix and complexity of an entity will dictate whether there are sufficient resources to implement an internal risk management function. The entity needs to determine whether the risk function can be undertaken internally or requires external support. In addition, consideration should be given as to whether an internal audit function is required and, if so, its interaction with the management of risk within the entity.

21 Australian Prudential Regulation Authority, *Prudential Standard CPS 220: Risk management*, p 9, January 2015: The role and responsibilities must be summarised in their risk management statements and it is also required that the risk management function is operationally independent. An APRA-regulated institution's chief risk officer must be independent from business lines, other revenue-generating responsibilities and the finance function. APRA-regulated entities are also required to ensure that the chief risk officer has a direct reporting line to the CEO, and regular and unfettered access to the board and the board risk committee.

A risk management function does not have to mean a team of people who sit in a room separate from the business. A sound risk management function should be embedded throughout the business. It can be difficult to make risk management 'come alive' for all employees in an organisation. It can seem esoteric or something with which only senior management needs to be concerned. Yet risk management is everyone's business, and is about making informed business decisions by creating awareness of risk. Figure 2 on the next page sets out, accessibly and clearly, how to continually maintain a risk register in the normal course of business.

Directors should retain focus that risk management performs both a control and a strategic function. Risk management is less effective in organisations where it operates purely as a control function.

Questions directors can ask about the risk management function

Directors are subject to liability and should maintain a high standard of governance, of which risk management is an essential component.

- How close to the business is the risk team? Is the team able to operate objectively?
- Are the terms used relevant and understood by everyone in the business?
- Does management retain accountability for managing risk?
- Do the board and the CEO provide a clear licence to the chief risk officer to assist divisions?
- Does the chief risk officer have a direct line of report to the audit or risk committee?
- Can the chief risk officer be fired by the CEO or other senior executives, or are they independent of the senior executive team?
- Is the risk management function given appropriate levels of authority, influence and independence in the organisation?
- Is there a single person or team responsible for coordinating risk across the organisation?
- Does the approach to risk management take into account risk scenarios and the interaction of multiple risks?
- What was the date of the last operational review of the risk management function by internal audit and what was the result and action taken by management?

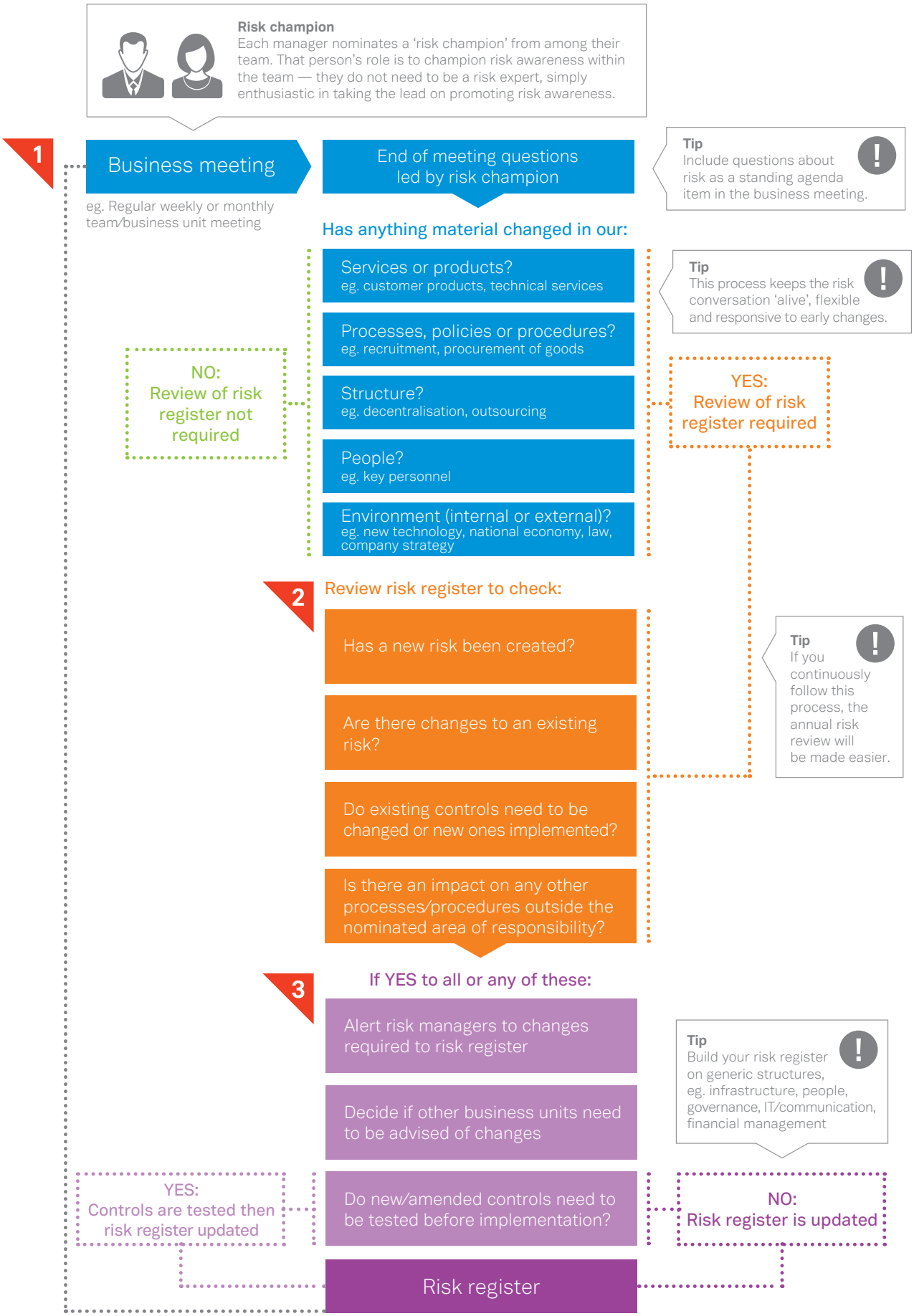
Reporting

The primary objective of contemporary risk reporting and analysis is to facilitate better risk management. In turn, the success of risk management should be measured by criteria that encompass the overall success of an organisation in areas such as:

- major decision-making in an environment of uncertainty
- shareholder/member value and performance
- good governance and enhanced reputation.

Against this background, risk reporting and analysis cannot take place in a narrow technical context. Modern risk reporting and analysis must be designed so that it is directly linked to and influences an organisation's core objectives.

Figure 2: Continual maintenance of risk register



The style and content of risk reporting and the tools to support it should be relevant to the nature of decisions that the board makes, for example, strategic risks; risks outside the risk appetite; and new and emerging risks. A useful starting point is for dialogue between the board and management, including the functional head of risk, to determine the nature of the decisions and stewardship that will be the focus of the board over a typical year. This dialogue should be refreshed at least annually. From there it will be possible to determine the risk reporting that management needs to develop and provide. This should cover the three elements of 'business as usual' stewardship, business cases and resulting project reporting, and material incident reporting.

Management needs to:

- determine the systems that are required to effectively monitor and manage risks
- ensure that any system accommodates a robust response mechanism
- determine the reporting systems and internal controls that are required to effectively report on risk and risk mitigation strategies (and assess whether the reporting is geared to actions and improvements rather than merely noting instances of concern)
- consider the advantages and disadvantages of a certification process and whether it is feasible to implement such a process, taking into account any regulatory requirements that the board of the organisation may have to meet
- assess whether the risk assessment data is robust
- consider training programs.

Some of the key business processes that must be aligned with risk reporting and analysis are the following:

- **Internal audit** — Internal audit reviews the effectiveness of controls. In terms of control assurance, this process should be based on critical functions and processes chosen on risk-based criteria.
- **Strategic planning** — Risk analysis is a key input to the strategic planning process of any organisation. Identifying risk as part of the business planning process enables strategies to be developed that actively address risks, and enables strategies to be avoided if the associated risks are unacceptable.
- **Performance management** — All risk responsibilities, whether a general responsibility to use the risk management processes or specific responsibilities such as risk ownership or risk mitigation initiatives, should form part of both organisational and individual performance plans.

Board reporting

Reporting of the risk management framework needs to be formally included in the board reports and listed as an agenda item of a frequency and regularity consistent with the risk appetite of the organisation so that the board can satisfy itself that the risk management framework continues to be sound.

Reporting of risk management programs and initiatives is primarily an aid to good governance. Reporting risk information should be for the purpose of informing board decision-making. This type of information provides assurance that the risk management processes and practices are effective, appropriately located in a functional sense, connected and relevant to the business and are being actively managed and improved.

The board should, as a minimum, consider the following issues, in evaluating its systems of internal control:

- the nature and extent of downside risks acceptable for the organisation to bear within its particular business
- the likelihood of such risks becoming a reality
- how unacceptable risks should be managed
- the organisation's ability to minimise the probability and impact on the business
- the costs and benefits of the risk and control activity undertaken
- the effectiveness of the risk management process
- the risk implications of board decisions.[22]

The new and emerging risks report provides an opportunity to highlight emerging risks or add new risks to the risk register throughout the year.

Risk escalation should occur within a defined policy context where there is a set of approved risk tolerances, or approved risk appetite guidelines, that serve as boundaries within which all risk exposures should remain. Risk escalation is an important tool for ensuring that risks are known and understood by the people with the authority to appropriately manage them.

If a risk exceeds approved tolerances or limits, poses an extreme threat or is likely to attract extreme external scrutiny or requires allocation of added resources, then it is normally not appropriate for it to be managed at the divisional level. At this point, an escalation process should be triggered under which the senior executive and the board and possibly external stakeholders are immediately informed.

Board papers

No business case should come to the board without competent risk assessment attached to the proposal. The risk assessment process, leading to advice on options ultimately for decision by the board, needs to include quantitative data that tracks the performance of management in implementing the board's agreed strategy. It should also include qualitative data, but not be dependent on that alone. The metrics and methodology used for the calibration of performance against the risk appetite should be matters for review and approval by the risk committee. It is essential that management and board have clarity as to the levers that need to be engaged to manage any identified risk to the value of the organisation.

It is important that the board has a clear view of the risks being assessed and understands the results, both good and bad. The board needs to have a high level of confidence in the tools being used to assess risk and the application of these.

Tools

Risk matrices are commonly adopted by the board and refined by management to assess risks within the business. The criteria used in the risk matrix should be suitable to the context of the organisation and consistent with its risk appetite.

Sophisticated risk management systems provide an array of quantitative statistics that can be a rich source of information for the organisation.

22 AIRMIC, ALARM and IRM 2002, *A Risk Management Standard*, section 9.2, UK

Indeed, there is a substantial toolbox of tried and tested techniques for the management and control of financial risk. However, they are dependent on the data fed into the system. If major risks are not being captured in the information being analysed, because they are not explicit or have not been considered, then any statistics gleaned from such systems will not assist the organisation to manage its risks effectively. The truism of 'garbage in, garbage out' applies to risk management tools, as the quality of the data being fed into the system and clarity as to the extent of understanding captured by the data is central to whether such a system will enhance the organisation's capacity to manage its risks or undermine it.

The benefit of sophisticated risk management systems and statistics is not that they are flawless, but in the imposition of a structured methodology for critically thinking about risk and acting on the results as required. Selection of quantitative data needs to be relevant to what the board needs to see to make informed decisions. The data needs to be both relevant and accurate.

Questions directors can ask about board reporting

- Are the elements of the risk management framework operating as intended and providing the benefits sought?
- How often does the board discuss risk with management?
- How is management addressing the major opportunities and risks facing the organisation?
- How does the board know that these are, in fact, the major opportunities and risks, and that the steps management is taking to address them are appropriate?
- What are the top 5–10 risks and mitigation strategies being monitored?
- What are the risks that are likely to result in a material misstatement in the annual financial statements?
- How does the board know when risks are increasing, holding steady, or decreasing?
- How is risk built into the business plan and strategy development?
- Is the hierarchy of risks still fit for purpose?
- Is there analysis from the perspective of key stakeholder groups (customers, staff, investors, regulators, communities) which could reveal areas of risk to ongoing viability that traditional analytical approaches may miss?
- Does the board have assurance that it is receiving the information it needs?
- What level of assurance does the board want?
- Are controls in place to investigate the quality of the information flowing to the board?
- Do all proposals come to the board not only with a business case but also risk assessment and does reporting on projects include risk reporting?
- Does the same discipline applied to the business-as-usual reporting apply to decisions concerning new projects?
- Is risk management integrated with all of the business's systems, such as performance management, process management and implementation of strategy?

Glossary

Governance: There is no one conclusive definition of corporate governance. The ASX Corporate Governance Council's *Corporate Governance Principles and Recommendations* define it as:[23]

> Corporate governance is 'the framework of rules, relationships, systems and processes within and by which authority is exercised and controlled in corporations'. It encompasses the mechanisms by which companies, and those in control, are held to account.

Other useful definitions of governance include that provided by the Organisation for Economic Co-operation and Development (OECD)[24]:

> Corporate governance involves a set of relationships between a company's management, its board, its shareholders and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined.

Board: The highest level of governing body charged with the responsibility to direct and/or oversee the activities and management of the organisation (it could be a group of directors as defined in corporations law; a set of trustees; the members of a management committee; or in the case of a government agency the head of that agency).

Culture: The shared attitudes (values) and behaviours of the individuals within the organisation. The culture is both a product of the attitudes and behaviours of individuals and an influence over them.

Director: The individuals who make up the governing body — the board (see above).

Key risk indicator: A type of performance indicator that highlights a change in exposure or a change in the likelihood of an event of interest — it measures a change in the internal or external environment; or deviations from a target result; and can reflect a desirable or undesirable changes. ISO:31000:2009 does not use the term.

Management: Those whose primary role is to manage or operate the entity on a day-to-day basis.

Risk acceptance: Informed decision to take a particular risk.

Risk appetite: The amount and type of risk that an organisation is willing to pursue or retain, sometimes referred to as 'risk tolerance' or 'risk attitude'.

Risk management: Framework set of components that provide the foundations of and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management.

Risk management policy: Statement of the overall intentions and direction of an organisation related to risk management.

Risk: The effect of uncertainty on objectives.

---

23 Justice Owen, HIH Royal Commission, *The Failure of HIH Insurance, Volume 1: A Corporate Collapse and Its Lessons*, Commonwealth of Australia, April 2003, pg xxxiii

24 Organisation for Economic Co-operation and Development, *G20/OECD Principles of Corporate Governance*, 2015, p 9

Governance Institute of Australia provides a range of professional development options for you, your board and management team including onsite training, world-class accredited postgraduate courses and short courses delivered face to face or online. For further information please contact your local Governance Institute of Australia state office.

New South Wales & ACT
T (02) 9223 5744
F (02) 9232 7174
E nsw@governanceinstitute.com.au

Queensland
T (07) 3229 6879
F (07) 3229 8444
E qld@governanceinstitute.com.au

South Australia & Northern Territory
T (08) 8132 0266
F (08) 8132 0822
E sa@governanceinstitute.com.au

Victoria & Tasmania
T (03) 9620 2488
F (03) 9620 2499
E vic@governanceinstitute.com.au

Western Australia
T (08) 9321 8777
F (08) 9321 8555
E wa@governanceinstitute.com.au

governanceinstitute.com.au

Governance Institute of Australia