Governance Institute of Australia

# Risk management for directors: A guide

Governance Institute of Australia 2022

# Table of Contents



Governance Institute of Australia

# About us

A national membership association, Governance Institute of Australia advocates for a community of more than 43,000 governance and risk management professionals, equipping our members with the tools to drive better governance within their organisation. We tailor our resources for members in the listed, unlisted and not-for-profit sectors, and ensure our member's voice is heard loudly. As the only Australian provider of chartered governance accreditation, we offer a range of short courses, certificates and postgraduate study to help further the knowledge and education of the fast-growing governance and risk management profession. We run a strong program of thought leadership, research projects and news publications and draw upon our membership of the Chartered Governance Institute to monitor emerging global trends and challenges to ensure our members are prepared. Our members know that governance is at the core of every organisation — and in these tumultuous times, that good governance is more important than ever before.

# What this guide covers

This resource has been developed by Governance Institute of Australia as part of its commitment to promoting good governance and risk management. It is designed to be a practical resource to assist Australian directors in any sector.

It is intended to assist boards to integrate and enhance their oversight of 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. It is not intended to advise directors about how to create an enterprise risk management system or a technical management-led risk process — these are more suited to development by management.

The original edition of the guide was published as *Risk Management: A handbook for directors* in 2016. This revised edition is published in 2022.

# Acknowledgements

Governance Institute acknowledges the contribution of Judith Fox FGIA, author of the first edition of this guide.

# Glossary

ACNC means the Australian Charities and Not-for-profits Commission which regulates charities.

ASIC means the Australian Securities and Investments Commission the corporate, markets, financial services and consumer credit regulator.

APRA means the Australian Prudential Regulated Authority the banking, insurance and superannuation regulator.

Business judgement rule the ability of directors to rely on section 180(2) of the Corporations Act in relation to their obligation to act with care and diligence under section 180(1) of the Corporations Act.

Corporations Act means the Corporations Act, 2001.

Corporate Governance Principles and Recommendations means the *Corporate Governance Principles and Recommendations*, 2019, 4th Edition, ASX Corporate Governance Council.

ESG means environmental, social, governance.

Net zero or Net zero emissions means achieving an overall balance between greenhouse gas emissions produced and greenhouse gas emissions taken out of the atmosphere.[1]

Safe harbour means a legal provision to reduce or eliminate legal or regulatory liability in certain situations as long as certain conditions are met, particularly section 588G of the Corporations Act

[1] See the Climate Council.

# 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. This guide has remained one of our most in demand resources since it was first published in 2016. Recent high-profile corporate events where risk management has often been highlighted as a failing, serve as a strong reminder of the importance of board oversight of risk management. The recent global pandemic, with its corresponding impacts on supply chains and its acceleration of new patterns of work and cyber security threats, has fundamentally challenged how boards identify, mitigate and monitor risk.

Shareholders, investors and members increasingly expect boards to demonstrate and publicly disclose effective oversight of risk management, especially on climate and cyber risks. Public sector entities with boards also face increasing scrutiny from parliaments, ministers, departments, integrity bodies, ombudsmen and auditors general. There is growing recognition that the board's ability to effectively manage and disclose risk impacts a wider array of stakeholders, including employees and the communities in which organisations operate. This heightened level of public scrutiny is illustrated by a 2020 Governance Institute survey that found 60 per cent of risk professionals consider brand or reputation damage to be among the top five risks facing organisations in the immediate future.[2]

This practical guide aims to equip new, existing and prospective directors to fulfil their duties. It is more than tick-box compliance or a long list of regulations – instead it aims to spark challenging questions in the minds of individual directors and healthy debate around the boardroom table.

This guide is designed to assist directors in all sectors. It is essential reading no matter whether you are a director of a listed or unlisted company, a not-for-profit organisation, or a public sector entity with a board, and regardless of size.

In the years since this guide was first published, Australian directors and their organisations have undeniably grown in risk maturity. Boards have become increasingly systematic and have adopted more structured risk management processes. They are benefiting from a more conscious assessment of the risks embedded in their daily operations, aided by advances in risk management techniques and technologies, although sectoral differences remain. The impact of royal commissions into financial services and aged care and APRA's prudential inquiry into CBA have also driven a heightened focus on risk management.

The challenge now is to continue this maturation in other areas such as culture and non-financial risks including cyber security – areas where the guide has a renewed focus.

This updated resource builds upon the original work of Judith Fox and has been revised by Governance Institute with valuable inputs from members who are risk management practitioners, company secretaries and senior members of the business and not-for-profit community.

Armed with this guide, a director is well placed to tackle this integral element of good governance that is critical to organisational success.

**Megan Motto**
CEO

**Pauline Vamos**
Chair

[2] Governance Institute of Australia, 2020, Risk Management Survey Report 2020, p. 32.

# An integrated approach to risk management is central to good governance

Governance codes and regulators place the management and oversight of risk at the centre of corporate governance and the role of the board in steering organisations, and for good reason. Failures of risk management often involve a weakness of governance, and vice versa.

Governance and risk should be seen as connected and integrated in a single framework.

**Risk management should be integrated with governance in a single framework for any organisation overseen by a board or other governing body. The board should put in place a structured, continuous process to identity, manage and respond to risk.**

### What is risk and risk management?

Risk-taking is what organisations do — it is part of every decision an organisation takes. Risk management standard ISO 31000 2018 defines risk as 'the effect of uncertainty on objectives' and risk management as 'coordinated activities to direct and control an organisation with regard to risk'.[3] Risk encompasses the opportunities to create value for the organisation (upside or opportunity risk) as well as the threats or hazards present and to be considered to ensure value is not compromised (downside risk), with recognition of the uncertainties attached to the opportunities and hazards alike. Organisations that manage risk well can limit the impact of threats and take advantage of opportunities.

Risk management is critical as it assists organisations in setting strategy, achieving objectives, making informed decisions and potentially avoiding loss events. It also protects customers and vulnerable stakeholders from harmful impacts, such as those investigated by the royal commissions into the financial services and aged care sectors.

Key elements of a risk management framework include:

- assessing the organisation's appetite and tolerance for risk
- clear and documented lines of responsibility and accountability for risk management and risk decisions
- a documented process for identifying types of events that could compromise the achievement of the organisation's objectives, as well as opportunities for value creation
- putting in place policies and processes to mitigate the identified risks
- monitoring and managing risks over time at an operational level
- establishing contingency plans for major risk events and emergencies that may occur, and
- regularly assessing the adequacy of the risk management framework.

## The regulatory environment

While by no means a new concept, risk management is the subject of increasing attention and regulatory activity in many jurisdictions. Australia is no exception. No sector is immune.

Directors face an increasingly complex array of national, state-based and international governance and risk management regulation, including a mix of mandatory, voluntary, principles-based and rules-based regimes. Some industries are more heavily regulated than others. Not all codes and regulations are aligned, and many vary in their level of detail about risk management.

These ever more stringent regulatory requirements have been influenced by local and global events. They include high-profile corporate collapses that led to the Sarbanes-Oxley regulation in the United States (2002), the 2008 global financial crisis, the Financial Services Royal Commission in Australia (2017-2019), the Royal Commission into Aged Care Quality and Safety (2018-2021), the growing consensus on climate change science, the rapid uptake of digital technology, the COVID-19 pandemic and global conflict.

[3] Standards Australia, 2018, *AS ISO 31000:2018*, < https://www.standards.org.au/standards-catalogue/sa-snz/publicsafety/ob-007/as--iso--31000-colon-2018 >.

**What this rapidly evolving regulatory environment underscores is the board's ultimate accountability for risk management and the importance of directors taking an integrated, organisation-wide perspective to the oversight of risk.**

Regulatory obligations on directors in relation to risk management include:

- directors' duties at common law, in the *Corporations Act* and under other statutes
- the ASX Corporate Governance Principles and Recommendations for listed companies
- ASIC, APRA and ATO standards, regulations and regulatory guidance
- the Privacy Act and notifiable data breaches to the Office of the Australian Information Commissioner
- emerging regulation around cyber security and the protection of critical infrastructure assets and assets of national importance
- environmental protection legislation
- anti-discrimination laws
- anti-money laundering laws
- whistleblowing legislation
- public sector governance legislation and standards applicable to public sector entities
- ACNC legislation and regulation applicable to charities and not-for-profits
- state and territory legislation applicable to incorporated associations
- workplace health and safety legislation and workers' compensation law.

Put simply, in addition to their duty to act in the best interests of the organisation, directors have other legal and fiduciary duties. To discharge these duties, directors must carefully oversee and, where appropriate, disclose the risks faced by the entity.

Directors of companies regulated by the Corporations Act have some protection from personal liability through the operation of the safe harbour provision, relating to claims for insolvent trading, and the business judgment rule, which protects directors from personal liability for poor decisions made in the course of performing their duties. However, these protections are unlikely to apply if directors do not take proactive steps to fulfill their duties. This underscores the need for directors to understand and take their duties in relation to risk management very seriously and for boards collectively to ensure there is a robust and integrated risk management and governance framework is in place and continually improved.

## Shareholder and member interest in board oversight of risk management

Listed entities in many jurisdictions are expected to apply the principles and practices in a governance code in the relevant jurisdiction or provide an explanation for why they have not done so.[4] Investors look to these disclosures to make decisions about the deployment of their capital investment. They 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 of unlisted organisations, while not necessarily seeking to make decisions about the deployment of a 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 will have an interest in the board's accountability in respect of its oversight of risk management within the entity. Integrity and central agencies such as auditors-general, public service commissions, ombudsmen, anticorruption bodies and departments of treasury 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.

[4] In Australia, the Australian Securities Exchange (ASX) Listing Rules require disclosure of the extent to which the corporate governance frameworks and practices of listed entities align with or differ from the Corporate Governance Principles and Recommendations, the 'if not, why not' regime.

**Key question for directors:**

- If your organisation was the subject of a Royal Commission or other significant external review what failings or weaknesses might it identify in your governance and risk management framework?
- How do you believe your organisation's senior management team would answer the above question?

# Distribution of responsibility

## The role of the board

Risk management begins and ends with the board. This is an oversight role, not involvement in the day-to-day managing of risk.

The board has overarching responsibility for setting the organisation's strategy and business model and the corresponding level of risk.

Setting strategy and managing risk are closely connected. The board sets the entity's risk appetite – the nature and extent of the risks it is prepared to take to achieve objectives. The board oversees the integrated risk management and governance framework and regularly satisfies itself that this remains sound. This involves putting in place a structured, continuous process to identify, manage and respond to risk and overseeing management's implementation of strategic and operational risk management.

There should be appropriate demarcation between the roles of the board and management. The board is not a 'rubber stamp'. It may reject or make changes to management's recommendations. The board does not give effect to the operational elements of the framework. Directors should exercise caution when setting aside any strongly expressed recommendations of management.

It may be appropriate for the board to temporarily intensify its supervision of management in response to major risk management events or at pivotal moments in the achievement of organisational objectives such as mergers and acquisitions and major digital transformation projects.

## Individual directors

Directors should be aware of their responsibilities and duties in relation to risk management. All directors on 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 their training and development needs to ensure 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.

The board needs an appropriate mix 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 represent the best interests of the organisation and its members as a whole rather than those of individual members or interest groups. However, it is the responsibility of all directors, not just independent non-executive directors, to exercise independent and active judgment.

Given the integral role of audit, risk and related board committees, it is vitally important that individual members of these committees devote sufficient time and care to their duties.

Directors should ensure they have sufficient time to meet the obligations of their role. Directors who sit on multiple boards and risk committees should ensure they have sufficient capacity, especially during periods of intense workload.

Directors should also consider how they personally contribute to promoting an effective and respectful boardroom culture. Effective directors foster a probing risk culture in the boardroom, balanced with discretion and respect.

Length of tenure may also be relevant a director's ability to effectively contribute to risk management. The Corporate Governance Principles and Recommendations recognise that lengthy tenure may pose a risk to director independence and the loss of opportunities for fresh ideas and perspective.[5]

## 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).

[5] See the discussion in ASX Corporate Governance Council (2019) Corporate Governance Principles and Recommendations, 4th Edition, ASX Corporate Governance Council, p 14. Recommendation 2.3.

There should be appropriate monitoring systems in place to provide assurance (safeguard) that decisions are being made in the right way for the right purpose.

The board needs to know that an effective framework is in place clarifying who is authorised to make what decisions and in what circumstances.

There should also be comprehensive delegated authorities in place, 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 delegation of authority is a key structure articulating risk tolerance in an 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 and therefore needs to be clear and easy for staff to use. Appropriate training is essential in ensuring that staff understand the operational limits of their delegation.

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 a particular authority is delegated.

The board and management need to ensure that all material risks, both financial and non-financial, are covered by the delegations of authority. A common weakness in delegations frameworks is that no senior executive is responsible for non-financial risks.

For APRA-regulated organisations the Banking Executive Accountability Regime (BEAR) establishes accountability obligations for banks and other authorised deposit-taking institutions and their directors and senior executives. BEAR will be replaced by the Financial Accountability Regime (FAR). FAR will extend strengthened, BEAR-like accountability requirements to other APRA-regulated entities and to their directors and senior executives with the aim of strengthening and increasing individual and entity level accountability across the financial services sector, including for non-financial conduct risk.

# Board committees – audit and risk

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

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

Perceived failings by audit and risk committees received particular attention in APRA's Prudential Inquiry into the Commonwealth Bank of Australia and the Final Report of the Hayne Royal Commission.[6] This underscores the need for the board to give careful attention to the structure, composition and functions of these committees, and for individual directors to give careful and full attention to their duties.

As with any board committee, audit and risk should operate under a written charter or terms of reference that clearly articulate the role, composition and specific responsibilities the committee will perform as well as any authorities that will be delegated. The composition and functions of these committees will depend on the particular circumstances of each entity, including its size, complexity and nature of its functions and operations. It is important to regularly review the composition of board committees to ensure there is an appropriate balance of the skills needed to carry out their work. This review is typically carried out annually by the committee chair with the assistance of the company secretary.

Since the first edition of this guide, there has been a gradual move towards separating risk management from audit. Governance Institute's 2020 risk survey found that dedicated risk committees were most common in ASX listed companies (40 per cent of respondents) compared to unlisted large businesses (27 per cent) and the government sector (27 per cent).[7] However, there remains no consensus about whether it is preferable to have a stand-alone audit committee and stand-alone risk committee, or to combine these committees. It is also possible to have no dedicated risk committee on the basis that risk management is the responsibility of every board and board committee.

The notable exception is where the committee structure is mandated. APRA requires APRA-regulated institutions to establish a board audit committee and a board risk committee. An audit committee is mandated in Australia for the top 500 companies under ASX Listing Rule 12.7. Principle 4 of the Corporate Governance Principles and Recommendations guidelines recommends all listed

[6] See *Prudential Inquiry into Commonwealth Bank of Australia*, APRA, 30 April 2018 at pages 16–17.
[7] Risk Management Survey Report 2020, Governance Institute of Australia, p. 16.

entities establish an audit committee, and Principle 7 recommends 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 an audit committee. By contrast a combined audit and risk committee is mandated for all NSW government departments and statutory bodies.[8]

Key considerations influencing committee structures include: resource constraints, whether combining audit and risk may bring clarity particularly where major risks are financial, and whether having separate committees will allow greater deliberation time. In a review of director oversight of non-financial risk, ASIC questioned what it perceived to be 'modest' meeting hours for risk committees at the institutions it reviewed that ranged from 16 to 40-hours a year across its sample.[9]

Many listed entities will have more than one board committee responsible for the oversight of different elements of risk, such as workplace health and safety, sustainability, investment, environmental impact and technology Given the rapid rise in cyber incidents during the COIVD-19 pandemic many organisations are reviewing which committee should have responsibility for cyber risk. Some organisations include cyber risk in the responsibilities of the audit and risk committee, others form a separate committee. Whichever approach is adopted the committee responsible needs to be satisfied that their organisations are sufficiently prepared to address this risk.[10]

It is essential to clarify the way 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. Audit and risk committees, where separate, should maintain a close working relationship to maintain consistency.

A board 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, and
- 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.

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.

## The role of management

It is management's role to recommend, execute and operate within the risk appetite, framework and process approved by the board, in line with the board's strategy and subject to its oversight.

Boards' expectations of senior management teams' involvement and attention to risk management are increasing.

Management should establish mechanisms to:

- monitor exposure and risk management performance — monitoring risk appetite at an organisational level means 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, and
- routinely monitor and evaluate the risk management processes and report to the board.

## Appointing and challenging management

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

Effective risk oversight begins with a clear, mutual understanding of the extent and nature of the board's responsibilities compared to those of management and other stakeholders. The ultimate goal is that boards have confidence in the information they receive from management, and management creates a cohesive process in which risks and their impacts are routinely identified, evaluated, and addressed. The assessment of risks to reputation and organisational long-term sustainability 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. Boards should periodically consider whether current management has the capacity to effectively manage risk, including as part of succession planning and executive remuneration policies.

The capacity of directors to bring independent judgment to bear on decision making and challenge executives is important in preventing domination of a board by any one individual — the CEO in particular. A culture of consensus, where management's recommendations are not questioned or challenged, is to be avoided especially at times of apparent business success. Such questioning relies on a clear understanding of the strategic risks and opportunities facing the organisation.

[8] NSW Treasury (2020) *Internal Audit and Risk Management Policy for the General Government Sector* (TPP20-08), p. 2.

[9] *Director and officer oversight of non-financial risk* report, ASIC Corporate Governance Taskforce, 2019 p. 43.

[10] See *Cyber Risk Readiness, Response & Ransom: An Audit Committee perspective*, The Institute of Internal Auditors Australia 2022.

The Financial Services Royal Commission highlighted the central importance of directors holding management to account.

> **Boards cannot operate properly without having the right information. And boards do not operate effectively if they do not challenge management.**
>
> Commissioner Kenneth Hayne[11]

## Chief Risk Officer

It is becoming more common for boards to identify an executive to lead the risk management process in order to promote accountability.

APRA-regulated entities are required to have a designated risk management function and must appoint a Chief Risk Officer (CRO) to be responsible for that function.

The CRO should report directly to the CEO and the CRO's office should be independent of all other business units. It may be beneficial for the CRO to have a clear and direct reporting line to the full board and/or the Audit/Risk board committee, to ensure an undiluted and non-conflicted 'voice' on risk is heard at board level. A dedicated CRO may also assist in embedding risk management processes more fully into the day-to-day operations of the organisation.

Whether or not a CRO is appointed, board expectations for increased CEO and senior management team involvement and attention to risk management are increasing.

## Dedicated risk management function

The organisation's size, business mix and complexity will dictate whether there are sufficient resources to implement an internal risk management function. This unit may report to a CRO or another senior executive.

A risk management function is responsible for designing and implementing the risk management framework that is appropriate for 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, the function needs to be structured and have a mandate to fulfil its role and accountabilities.

The risk management function needs to be sufficiently close to the business to properly advise the business, rather than housed in a separate silo. At the same time the risk management function must not be 'captured' by the business functions and must retain sufficient independence to fulfill its assurance function, question the decisions of other business units and, if necessary, escalate concerns. Each organisation needs to decide the appropriate balance between these two aspects of its function. In large organisations these functions may be separate roles and held by different individuals, but this may not be the case in smaller organisations.

Directors should remember 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.

If the organisation has an internal risk management function and an internal audit function, consideration should be given by the board to the interaction between these two functions within the entity.

**Key question for directors about the risk management function:**

- 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 CRO to assist divisions?
- Does the CRO have a direct line of report to the audit or risk committee?
- Can the CEO terminate the employment of the CRO or other senior executives, or are they independent of the senior executive team?
- Does the risk management function have an appropriate level of authority, influence and independence in the organisation?
- Does the risk management function have adequate resources and skills to undertake its role?
- 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?

[11] Final Report, Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, Commissioner Kenneth Hayne, 2019, Volume 1, p. 396.

## Internal audit and external audit

A board needs to satisfy itself that the risk management framework is operating effectively and as intended. Effectiveness can be tested from time to time through assurance providers such as internal or external audit.

A listed entity should disclose if it has an internal audit function, how that function is structured and what role it performs. If it does not have an internal audit function it should disclose the processes it employs for evaluating and improving the effectiveness of its governance, risk management and internal control processes.[12]

An internal audit function brings a systematic, disciplined approach to evaluating and continually improving the effectiveness of an organisation's risk management and internal control processes. An internal function has a unique role in that it is based inside the organisation, but is also independent and objective. Its knowledge of practices across an organisation also mean it is well placed to provide a perspective on organisational practices and risk culture based on its observations of practices and behaviours. The head of the internal audit function should have a direct reporting line to the board or to the board audit committee, and risk committee or committees if they are 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. Smaller organisations frequently engage an external consultant to provide independent internal audit services. The board may see advantages to using external consultants to support the internal audit function, or in outsourcing the internal audit function.

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 committees are not included in the 'three lines of defence' but are served by the 'three lines'. Its role is to ensure that the 'three lines of defence' model is reflected in the organisation's risk management and control processes.

It is important that there is a good understanding of the three lines of defence throughout the organisation.[13] [14]

Boards should also be aware that regulators have in recent years intensified their focus on audit quality.

## Line managers and frontline employees

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.

In most large organisations, there will be a person or team responsible for the design, implementation and monitoring of adherence to the risk management framework who can also act as a 'single point of reference' regarding risk and threat management. The seniority of the head of risk management varies. However, there is rarely a single person or team responsible for coordinating the information about risk across the organisation and synthesising that information for the board. Usually, different teams for example, finance, operations, public relations, executives, manage 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 these risks either align with or diverge 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 organisation's products and services.

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, and
- 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.

[12] See Recommendation 7.3 Corporate Governance Principles and Recommendations.
[13] See for example, *Report Board Governance of AML/CTF Obligations at Westpac: The Advisory Panel Review*, 8 May 2020 at p 14.
[14] See also The IAA Three Lines of Defence Model, July 2020.

**Questions for directors:**

- 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?
- 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 a CRO in a larger organisation or the chief financial officer or company secretary in a smaller 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?

## ESG risks

There is increasing pressure from shareholders and other stakeholders for corporate action and disclosure on ESG issues. These often involve a risk management component, including requests for climate change risk disclosures, genuine commitments to achieve net zero targets, and divestment from fossil fuel assets.

Social risks to consider include workplace bullying, sexual harassment and assault, geopolitical risks, demographic risks as Australia's population ages, issues affecting cultural minorities, and ethical risks such as corruption and human slavery in global and domestic supply chains.

Governance relates to the governance of organisations and many investors focus on governance issues because they consider it impacts the value of their investment.

## Climate change risk

Climate change poses significant challenges for Australia, affecting its society, economy and natural environment. Australia is particularly vulnerable to drought and bushfires, which may be exacerbated by climate change. It has historically relied heavily on fossil fuels for energy security and economic growth. Climate change also poses challenges for biodiversity. Investors and other stakeholders such as regulators are increasingly seeking disclosure from organisations about their exposure to, and management of climate change risk. There is also increasing regulatory focus on climate change risk. In 2021 alone:

- ASIC committed to targeting misleading ESG claims related to financial products as part of their 2021-2025 corporate plan and warned of regulatory action against misleading net-zero claims.[15]
- APRA commenced its climate vulnerability assessment on the five largest Australian banks to help assess the vulnerability of institutions and how they may adjust their business models in response to climate change.

In 2021 Noel Hutley SC and Sebastian Hartford-Davies updated their 2016 opinion on climate change. In their 2016 opinion they expressed the view that directors' duty of care and diligence under the Corporations Act permits or requires Australian company directors to respond to climate change risks. Their view was that directors who failed to who failed to consider climate change risks then could be found liable for breaching their duty of care in the future. In 2021 they say it is 'clear the benchmark for directors on climate change and attendant risks and opportunities continues to rise'.[16]

[15] See Speech, *ASIC's Corporate Governance Priorities and the Year Ahead*, ASIC Chair Joe Longo, 3 March 2022.

[16] See *Climate Change and Directors' Duties, Further Supplementary Memorandum of Opinion*, Noel Hutley SC and Sebastian Hartford-Davies, 23 April 2021.

In recent years many organisations have announced net zero targets. Since the United Nations Conference on Climate Change – COP 26 the number is likely to increase.[17]

Climate change risk will impact organisations in all sectors either because of their own operations or because it impacts their suppliers, customers and other stakeholders. For these reasons directors should consider the impact of climate change on their organisation and consider appropriate disclosures. The Task Force on Climate-related Financial Disclosure (TCFD) framework is rapidly emerging as the preferred framework for disclosure of material climate-related risks.[18] In 2022 the International Sustainability Standards Board was formed to develop comparable reporting by companies on climate and other ESG issues.

There has also been a significant increase in climate change related litigation. Globally, the cumulative number of climate change-related cases has more than doubled since 2015.[19] This represents an increasing risk for organisations in all sectors.

## Nature loss

There is also an increasing focus on the financial risks that nature loss poses for organisations. The Task Force on Nature-related Financial Disclosure (TNFD) is a global, market-led initiative with a mission to develop and deliver a risk management and disclosure framework for organisations to report and act on evolving nature-related risks. The TNFD Framework draws on the TCFD Framework recommendations with recommended disclosures covering four areas: governance, strategy, risk management and metrics and targets. The final TNFD recommendations are scheduled for release in 2023.

## Social risks

Investors and other stakeholders have an increasing interest in how organisations are managing a group of risks characterised as 'social risks — the potential negative risks to organisations that result from their impacts on communities of people such as employees, customers and local communities. A number of well documented failures to manage these risks have lead to significant reputational and other damage to a number of public and private sector organisations.

Social risks include:

- Modern slavery – this includes serious exploitation such as trafficking in persons, slavery, servitude, forced marriage, forced labour, debt bondage, the worst forms of child labour and deceptive recruiting for labour or services.[20] It is important for organisations to identify modern slavery risk and proactively address the risks identified including risks across their supply chains.
- Human rights – this relates to the human rights of people organisations impact, including in their workforces, communities, customers and end-users. Poor practices can expose organisations to significant reputational and financial risk.
- Poor labour standards – there have been a number of high-profile scandals relating to underpayment of staff. There are also growing risks relating to casual and insecure employment and unsafe working conditions.
- Workplace safety – The safety of a workforce not only relates to physical safety, but also to mental health, and organisations should ensure that there is adequate support for employees' psychosocial wellbeing. Ensuring workplaces are free of sexual harassment is an increasingly fundamental part of providing a safe workplace for all employees. Safety also extends to proactively preventing and responding effectively to racism and other forms of discrimination
- Diversity – Organisations are likely to be more successful when they harness collective intelligence and approach problems with cognitive diversity. There are a several aspects of diversity which organisations may wish to consider when looking at diversity. They include: gender, age, education and professional experience and ethnicity. There has also been a focus for some years on increasing gender diversity on boards and in senior management teams, particularly for listed companies.

[17] See A Guide for board and management on the path to net zero, Governance Institute of Australia, 2022.

[18] See Climate Change Risk Disclosure: A practical guide to reporting against the Corporate Governance Principles and Recommendations, Governance Institute of Australia, 2020.

[19] See Setzer, J., Higham, C., *Climate change litigation is growing and targeting companies in different sectors*, 2021.

[20] See section 3 Modern Slavery Act 2018 (Commonwealth).

## Governance risks

Governance risks relate to the risks that arise from poor governance practices. Good governance is important to shareholders, stakeholders, employees and customers alike and has a strong link to an organisation's reputation. Poor governance practices are therefore a source of risk for organisations.

Governance Institute considers governance has four key components:

- Transparency – making clear disclosures about the organisation's structure, operations and performance, both externally and internally, and maintaining a genuine dialogue with, and providing insight to, legitimate stakeholders and the market generally.
- Accountability – ensuring that there is clarity of decision-making within the organisation, with processes in place to ensure that the right people have the right authority for the organisation to make effective and efficient decisions, with appropriate consequences for failures to follow those processes.
- Stewardship – developing and maintaining an enterprise-wide recognition that the organisation is managed for the benefit of its shareholders/members, taking reasonable account of the interests of other legitimate stakeholders.
- Integrity – developing and maintaining a culture committed to ethical behaviour and compliance with the law.[21]

Recognising and managing risk is a crucial part of the role of the board and management and oversight of risk management is the responsibility of the board. Risk management is an important part of governance.

In Australia, the principal reference and reliance for corporate governance rests in the provisions of the *Corporations Act 2001* and the Corporate Governance Principles and Recommendations.

Good governance therefore ensures transparency and accountability, and can prevent scandals, fraud and issues relating to organisational liability. An organisation that bases its structure and corporate culture on good governance principles is more likely to avoid major disasters.

## Technology risks

While technology business units and service providers for an organisation should have an active risk register and risk management approach and culture, technology risks can also significantly impact overall organisational performance, customer experience and reputation. It is therefore advisable for organisations to establish a process and criteria for how technology-related risks of strategic or widespread operational impact can be included or escalated to the appropriate governance and overall risk management levels within an organisation.

## Cyber risk

Given the increased amount of global online activity during the recent pandemic combined with a significant escalation in global conflict, the number of cyber-attacks has increased dramatically. Consequently, organisations and their boards have a heightened focus on this risk. At the same time this increase in global online activity has also been a source of opportunity for many organisations, opening up new products and markets and increasing their ability to connect to their stakeholders.

Many organisations use the Australian Cyber Security Centre's Essential Eight Maturity Model as a first step towards improved their cyber security risk profile.[22]

A recent Federal Court decision found that a company which held an Australian Financial Services Licence was in breach of the provisions of the Corporations Act due to conduct involving cybersecurity.[23] This is the first case in which ASIC has exercised its powers for an organisation's failure to have adequate cybersecurity and cyber resilience risk management controls. While this case relates to an ASIC regulated financial services firm it is also relevant for other organisations which may come under scrutiny by other regulators because they are subject to similar obligations.[24] They need to ensure there is a robust monitoring of incidents to proactively identify broader systemic issues or system deficiencies and that there is no delay in developing and implementing improved compliance measures once a deficiency has been identified.

ASIC's good practice guidance for financial services firms encouraging activity to promote cyber resilience also serves as a useful starting point for organisations in other sectors. ASIC considers that 'informed oversight of risk involves the board being satisfied that cyber risks are adequately addressed by the risk management framework of the organisation. Important controls include ensuring the organisation has appropriate safeguards in place against malicious cyber activities, and that recovery capabilities are adequate'.[25] ASIC's questions below are a useful guide for boards when considering the management of cyber risk.

[21] See Governance Foundations at www.governanceinstitute.com.au.
[22] See Issues in Focus Cyber Risk, The Insurance Council of Australia.
[23] See ASIC v RI Advice Group Pty Ltd [2022] FCA 496.
[24] See also *What a Federal Court ruling on cybersecurity means for AFS licensees*, ASIC 2022.
[25] See *Key Questions for an organisation's board of directors*, at www.asic.gov.au.

## Questions for directors on cyber risk

**Risk management framework**

- Are cyber risks an integral part of the organisation's risk management framework?
- How often is the cyber resilience program reviewed at the board level?
- What risk is posed by cyber threats to the organisation's business?
- Does the board need further expertise to understand the risk?

**Monitoring cyber risk**

- How can cyber risk be monitored and what escalation triggers should be adopted?

**Controls**

- What is the people strategy around cybersecurity?
- What is in place to protect critical information assets?

**Response**

- What needs to occur in the event of a breach? Boards should ask themselves:
  - » If and when a problem arises, what processes are in place for communicating effectively, internally and externally, and managing the situation?
  - » Has there been a sufficient level of scenario planning and testing to ensure that response plans are valid and up to date, including with third-party suppliers and dependants?[26]

Following a pilot assessment against the requirements of Prudential Standard CPS 234 Information Security APRA wrote to all APRA-regulated entities about boards' need to strengthen their ability to oversee cyber resilience. It expressed the view that it 'expects boards to have the same level of confidence in reviewing and challenging information security issues as they do when governing other business issues'.[27]

# Culture

The concepts of risk culture and organisational culture are closely interconnected.

It is APRA's view, adopted in this guide, that risk culture is 'not separate to organisational culture, but reflects the influence of organisational culture on how risks are managed'.[28] An organisation's culture is the sum of its shared values and behaviours. Applying APRA's view, organisational culture includes the values and behaviours of its people as they relate to various dimensions, such as risk, but that those dimensions are not separate cultures. References are commonly made to an organisation's innovation culture, safety culture or compliance culture — these would, under APRA's interpretation, simply be considered dimensions of the organisation's culture. However, there are alternate views that consider an organisation's risk culture to be separate from its organisational culture, rather than a subset of it. An example would be an organisation that, overall, has a positive culture and yet is deficient in the area of risk management.

Noting these range of views, it can be stated confidently that an organisation's culture influences — positively or negatively — how it manages and tolerates risk, and that in turn the risk culture is capable of shaping the organisational culture.

> **'…the culture of an entity can be described as 'the shared values and norms that shape behaviours and mindsets' within the entity. It is what people do when no-one is watching…'**
>
> Commissioner Kenneth Hayne[29]

It is also widely accepted that a robust risk management framework is beneficial to a healthy corporate culture as it drives accountability. Equally, risk immaturity in an organisation can fail to curb or exacerbate key conduct risks that contribute to negative impacts on the achievement of the organisation's objectives and detrimental impacts on stakeholders.

[26] Loc cit.

[27] See *Insight Improving cyber resilience: the role boards need to play*, APRA 23 November 2021.

[28] APRA, 2016, *Information Paper: Risk culture*, p. 7.

[29] Commissioner Kenneth Hayne, Final Report, Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry (2019) Volume 1, p. 334.

## The board's role in culture

The board is responsible for defining an organisation's purpose and approving its statement of values and the code of conduct to underpin the desired organisational culture.

A code of conduct reflects the core values of an organisation and the expectations of stakeholders and the community at large. But simply having the code is not sufficient — regular staff training and occasional updating of the code are also needed.

A key component of culture is the behaviour and conduct of senior managers and the board itself. This is often referred to as the 'tone at the top'. The organisation's clearly articulated ethical and behavioural standards must be reinforced in practice by the organisation's leadership group. The board and management must model, and must be seen to model, the desired culture as employees will follow the example of senior leaders. A number of recent well-documented scandals relating workplace sexual misconduct underscores the importance of 'tone at the top'.[30]

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 disconnect between the desired and stated culture and the actual culture, for it is only the actual culture — the enacted values — that ultimately matters.

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 take place. Both go to the heart of governance and risk management if they are to create and protect value for the organisation.

**The challenge for the board is to go beyond risk being a tick-box compliance exercise to develop an organisational culture where risk is genuinely considered and managed at all levels of the organisation.**

## Risk-aware culture

The risk culture of an organisation is the shared attitudes (values) and behaviours of individuals about the management of threats and 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.

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.[31]

## Incentives

Incentives play a powerful role in influencing individual's' values and behaviour and hence the culture. Incentives may have unintended consequences. Research has shown that individuals will seek to do those things that are rewarded, implicitly or explicitly, tangibly or intangibly, 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.[32]

[30] See for example, Set the Standard: Report on the Independent Review into Commonwealth Parliamentary Workplaces, Australian Human Rights Commission, November 2021.

[31] 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.

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