Diligent

Putting the G into Risk Governance

Introduction

Sound risk management is critical to the achievement of business success more than ever before. For directors, this starts with ensuring that risk governance across the organisation is set up for success. This White Paper focuses on the important features of effective risk governance for directors

Risk management has come to the forefront of directors' consciousness in recent years. In addition to the onset of the COVID-19 pandemic in early 2020, a range of new and challenging risks have emerged from the digitalisation of many business processes and the rise of cyber security threats. The convergence of these factors has elevated the conversations about risk management around the board table. Increased stakeholder expectations around risk governance coupled with the external environment are driving fundamental changes in the management of risk. Directors have had to stare into how their boards manage risk and are reassessing their risk management governance and oversight practices.

The emergence of the ESG (Environment, Social and Governance) movement is also seeing a renewed focus on risk governance. Risk management cuts across each of the three pillars of ESG. Under **Environmental**, questions must be asked about the risk profile of the organisation based on an assessment of the long-term impact of climate change. Organisations need to reassess business plans and strategies considering the impact of climate change on its current businesses. Under the **Social** pillar, in addition to the broad social responsibility lens that is applied to a business' activities there are a myriad of specific compliance requirements in areas that include privacy and data security, modern day slavery, employment practices, and anti-discrimination. The third pillar of ESG, **Governance** has many facets to it and sound risk governance and risk management is critical to meeting stakeholders' expectations under this pillar.

How should directors look to put the G into Risk Governance? For more heavily regulated businesses in industries such as healthcare and medicine, utilities or financial services, there are often prescriptive requirements for risk management. This may include detailed governance, risk, and compliance requirements. However, for less regulated or unregulated sectors, risk governance is often harder to define. It can be difficult for directors to be satisfied that risk governance is both effective and fit for purpose.

Many boards still discuss risk management matters infrequently and in an unstructured manner. For some boards, the agenda item for risk management is tucked away in an operational, legal or finance report. Fortunately, many organisations now have dedicated board subcommittees to guide them. This will usually be a dedicated risk committee or a combined audit and risk committee.

Setting up an organisation for success in managing risk requires more than simply establishing a dedicated board subcommittee, however. A committee structure alone is not sufficient. Directors need to ensure that their boards and committees are taking a holistic and comprehensive approach to the governance and management of risk.

There are many aspects of risk governance and management that require close attention of boards. Below are the key areas for directors to focus on.

Risk Governance at the Board Level

The establishment of risk governance for an organisation starts at the board level. Whilst the board will delegate a range of risk management activities, duties and responsibilities under its delegations framework, it will always remain responsible for risk management. Even with a risk committee (or a combined audit and risk committee) the buck stops with the board.

The keys to effective risk management governance at the board level are:

- **Agreeing roles and responsibilities**
- **Establishing a board subcommittee (if desired)**
- **Approving an effective committee charter outlining how it oversees and reports on risk management**
- **Ensuring there are sufficient risk management skills and experience at board level**
- **Ensuring the board and any risk committee regularly reviews the design and effectiveness of the organisation's approach to managing risk**

The board charter will need to set out the board's specific role in the governance of risk management. Should there be a specific board risk subcommittee, then the board charter will need to be tailored to reflect that this committee is delegated responsibility to undertake certain responsibilities on behalf of the board. The risk committee's charter should, in turn, reflect this delegation of responsibility.

Smaller organisations will often have a merged audit and risk committee. This can be an efficient way of dealing with both audit and risk matters. It is important, however, to ensure that there is sufficient time devoted to both audit and risk matters. It can also be helpful for the committee to set aside some time each year to assess its effectiveness in carrying out the duties delegated to it by the board. Any external, independent review of board effectiveness will often also look at the operation of board subcommittees.

"For a non-executive director, making reasonable and impartial business judgements in the best interests of the organisation and shareholders within the qualitative and quantitative limits of the overall risk appetite is a fundamental accountability.

Whilst the traditional financial and non-financial risk dimensions remain front of mind, in 2021, security risk, process integrity and availability practices, and controls demand greater vigilance, as bad actors take advantage of the pandemic's impact and changing business conditions to exploit systems' vulnerabilities."

Jason Millett, Non-Executive Director,
Hay Limited and former CIO

Board Risk Governance Resources

Read: ASX Corporate Governance Council's Corporate Governance Principles and Recommendations (4th Edition February 2019)

Read: ASIC Corporate Governance Taskforce: Director and Officer Oversight of Non-Financial Risk Report

Read: Governance Institute – Resources Centre

With the increasing focus on the governance and management of risk by external stakeholders, it is important for boards to critically assess the collective skills and expertise of the board.

The ASX Corporate Governance Council's Corporate Governance Principles and Recommendations (4th Edition February 2019)[1] recommends that a board 'skills matrix' be utilised. It states that a board skills matrix is a tool "that can help the board identify any gaps in its collective skills that should be addressed by providing professional development to existing directors or taking on new directors." Recommendation 2.2 goes on to recommend that a "board should regularly review its skills matrix to make sure it covers the skills needed to address existing and emerging business and governance issues relevant to the entity."

The dynamic, interconnected environment that organisations operate in and the move to more digitally enabled businesses in this world give rise to many new risks. This is driving the need for new skills at board level – particularly in technology risk areas such as information security, cyber security, and information technology risks. In addition, business partner, supply chain, outsourcing and third-party vendor risks are increasingly prevalent in all businesses. Social media is also becoming an increasingly important area of focus from a risk perspective.

Fortunately, many organisations now have a skills matrix in place to assist directors assess the adequacy of the skills and expertise of the board and identity any skills gaps. It is critical for the skills matrix to be reviewed frequently. Directors should ensure that the are being honest around the existing board capability and skills and identify areas of weakness. It is also incumbent on directors to make plans to supplement the existing board with new directors to address any skill gaps in risk management areas.

Questions to ask

1. **Is there clarity on how risk is governed, at both board and management level?**
2. **Is there a need for a dedicated risk management committee?**
3. **Are there sufficient risk management skills and expertise around the board table?**
4. **Is there are board skills matrix in place? Does it include all areas of expertise that is needed to manage risk?**
5. **If there is a risk management committee in place, does it meet frequently enough?**

[1] https://www.asx.com.au/documents/regulation/cgc-principles-and-recommendations-fourth-edn.pdf

Risk Management Strategy, Frameworks and Processes

One of the most important roles the board (and any risk management committee) has is to develop and approve the organisation's approach to the management of risk. The key decision for the organisation is whether to adopt a formal Enterprise Risk Management (ERM) framework. ERM is a well-developed methodology for organisations to manage risks. It encompasses the identification, assessment, and management of risk. Formal risk management frameworks – even in a small organisation – can reduce operational losses, build confidence in the organisation, and assist it achieve its long-term strategic goals.

The ERM approach is documented in a core document usually referred to as a Risk Management Framework. It may also be referred to as the Risk Management Strategy. The Risk Management Framework (or Strategy) document will detail, as a minimum:

- **The governance of risk (including a summary of the roles and responsibilities)**
- **Processes for risk identification, risk measurement and assessment and risk mitigation**
- **Risk reporting, monitoring and escalation**

The Risk Management Framework will often also summarise the key business risks facing the organisation and its risk appetite (this is covered later in this paper).

The Risk Management Framework should be reviewed annually. Changes to the Risk Management Framework should be made to reflect changes in the organisation, changes in the external environment, or changes to the approach to the management of risk by the organisation.

These changes may be driven by organisational restructuring (for example, changes in management roles and responsibilities) or mergers and acquisitions activity.

The detail in the risk management frameworks vary considerately from organisation to organisation. Even in more heavily regulated industries, the approach, methodology and tools required to put in place is often not prescribed in detail by the relevant legislation.

> "Incoming directors may find risk is not significantly profiled in induction and they will need to request background documents, past reports, attend audit and risk committee meetings, ask questions, get briefed. It is also critical that directors be proactive informing themselves on new trends, research and expertise on risk; and for that reading and understanding to inform your contribution to the organisation's risk governance"
>
> **Kyl Murphy, Non-Executive Director,**
> South Bank Corporation Limited

Risk Management Frameworks and Industry Guides

Read: ISO 31000:2018 Risk Management — Guidelines, International Organization for Standardization

Read: Enterprise Risk Management: Integrating with Strategy and Performance (Executive Summary), Committee of Sponsoring Organizations of the Treadway Commission

Read: Risk management for directors: A handbook (April 2016), Governance Institute

Risk management frameworks do follow several well-known approaches, however. The global industry standard is known as ISO 31000:2018, published by the International Organization for Standardization[2]. Another well-known industry approach is the guidance outlined in the documents titled "Enterprise Risk Management — Integrated Framework" published by the US based, Committee of Sponsoring Organizations of the Treadway Commission (known as COSO)[3]. These industry guides and frameworks are a starting point for organisations seeking to implement an ERM approach for the first time. Directors should, as part of their personal professional development, familiarise themselves with these industry standards.

Questions to ask

1. Does the organisation have a documented approach to risk management?
2. Is there sufficient clarity on the roles and responsibilities across the organisation on risk management?
3. Does the board or risk committee receive reports from management on the effectiveness of the risk management frameworks and processes?
4. Have the organisation's risk management frameworks and practices been independently reviewed recently?
5. Are there risks arising that are not adequately addressed or covered in the risk management framework?

[2] https://www.iso.org/iso-31000-risk-management.html
[3] https://www.coso.org/pages/erm-integratedframework.aspx

Risk Identification, Risk Appetite and Key Risk Indicators

A crucial role for directors is to ensure that the organisation's key material business risks are identified, the organisation's appetite for risk taking in these areas defined, and that the directors have oversight of the management of these risks.

For a smaller organisation such a not-for-profit enterprise or privately owned small businesses, it may not be necessary to define risk appetite for many (or even all) risks in the business. Indeed, such businesses may have a very short list of business risks. For example, a not-for-profit industry association or charity that does not undertake any substantial commercial activities will have a very different risk profile to a not-for-profit enterprise with trading activities, suppliers, employees and customers. The Risk Management Framework will define the approach to risk management based on an assessment of the risk profile of the organisation and the risk management oversight determined by the board, taking into account the size and nature of the business.

For organisations that need to (or choose to) define risk appetite for its material business risks, the process will involve:

- **Identifying the material business risks**
- **Understanding the likelihood and consequence of the risks occurring**
- **Once the impact of the potential risks is understood, agreeing the appetite the organisation has for each specific risk**

Following this initial exercise, it is common to define risk appetite in a written, board approved document referred to as a Risk Appetite Statement. A Risk Appetite Statement is a board approved document that considers the material or most significant risks to which the organisation is exposed, its appetite for each material business risk, and the approach to managing these risks.

In its paper titled "ERM – Understanding and Communicating Risk Appetite"[4], COSO states that risk appetite is "the amount of risk, on a broad level, an organisation (sic) is willing to accept in pursuit of value. Each organisation pursues various objectives to add value and should broadly understand the risk it is willing to undertake in doing so."

> "It is important for risk committees and boards to consider carefully what information they need from management to enable them to properly perform their oversight function. This helps to ensure management are clear about what needs to be delivered and to then deliver information and reporting to demonstrate that risk management processes are working in alignment with the risk framework that is in place and has been approved by the Board, and that issues and challenges are being reported/discussed as well"
>
> **Karen Smith-Pomeroy, Non-Executive Director,** Kina Securities Limited

[4] https://www.coso.org/Documents/ERM-Understanding-and-Communicating-Risk-Appetite.pdf

The organisation's strategic plan and accompanying detailed business plans, developed, and implemented by management, will be consistent with the Risk Appetite Statement. It is important for directors to periodically review (and received assurances on) that risk appetite is being effectively incorporated into management decisions.

It also common for many organisations – particularly larger businesses – to establish a set of specific risk metrics, referred to as Key Risk Indicators, that assist board and management in assessing if the business outcomes are in line with the organisation's risk appetite. If KRIs are in place it is imperative that the board or risk committee receives reports from management on a regular basis on the performance against these measures.

Questions to ask

1. Does the board or risk committee regularly review its universe of business risks and the management thereof?
2. When did the board or risk subcommittee last dedicate time to undertaking an enterprise wise risk identification workshop?
3. Is risk appetite defined and well understood by the board and management?
4. Does the organisation need to develop a set of Key Risk Indicators to monitor the risk profile of the organisation, if not in place?
5. Does the risk management committee regularly report back to the board on the organisation's risk profile, in a structured and consistent manner?

Risk Resourcing and Capability

Any well-designed risk management framework needs to be fully implemented and assessed periodically for effectiveness. Boards often devote considerable time to risk management, establishing well thought-out, defined frameworks and processes only to later see them 'left on the shelf'.

Common reasons for risk management frameworks failing to become embedded can include insufficient dedicated risk personnel, budgetary or financial constraints, or a lack of appreciation by management of the importance of risk management. Certain risk responsibilities can often also be assigned to roles that have other competing business priorities.

The board and any risk committee should understand the primary ownership of risk management within the organisation and the design of the organisational structure. Directors need to be confident that the risk management frameworks are capable of being implemented. For larger organisations, it will be important to agree with management if a dedicated risk management function is required and its reporting lines. It is also increasingly common for medium sized organisations to have dedicated Head of Risk Management or Chief Risk Officer

It is also important for directors to challenge management on the adequacy of risk resourcing and regularly confirm that sufficient financial resources have been allocated to risk management.

Questions to ask

1. Are there adequate personnel in place – with sufficient authority – to oversee risk management in the organisation?
2. Is there a sufficiently senior person that regularly presents to the board or risk committee on risk management matters?
3. Does the organisation need a senior risk officer, such as a Head of Risk Management or Chief Risk Officer to be appointed to effectively manage its risks?
4. Does the board or risk committee formally review or discuss the adequacy of the resourcing of risk management in the organisation?

Governance, Agility and Emerging Risks

Maintaining agility whilst operating in line with the governance arrangements established can been challenging for directors. Risk committee meetings may only be scheduled to be held three or four times a year. In addition, meetings can often be deferred or cancelled for reasons outside the control of the directors.

Critical to success will be having a disciplined approach to the risk content of the agenda of each board or risk committee meeting. There should be a rolling agenda tabled at each meeting outlining the schedule for at least the next twelve months. This rolling agenda should be developed by the chair of the board or risk committee and reviewed by all directors and committee members.

It is also important that risk management reporting to the board covers a wide range of risk issues. The risk reporting needs to address known, existing business risks that have been identified and new or emerging risk issues.

Each meeting agenda should also have a standing agenda item for matters considered outside of the board or committee since the last meeting. In between meetings, risks issues may also arise and be escalated by management to the board for socialisation, review and/or discussion. Directors need to make themselves available for briefings on these issues and consider the matters presented. It is equally important to have these discussions documented and closed out, as necessary, at a subsequent meeting.

> "We need focused risk committees working with management to do the deeper risk work and make recommendations to the Board. A twice-yearly report from the Audit & Risk Committee appending an updated lengthy risk register for discussion at the end of a long board meeting is insufficient, in perpetually challenging and astonishing times."

David Shortland, Non-Executive Director,
ChildFund Australia and Governance Specialist

Questions to ask

1. Is the board or risk committee satisfied that the management reporting covers all business risks in sufficient depth and in a timely manner?
2. Is there a rolling agenda in place covering scheduled risk matters for future meetings?
3. Is the board or risk committee regularly discussing emerging risks?
4. Are risks issues escalated in a timely manner in between formal board or committee meetings?
5. Is there an agreed protocol for 'closing the loop' on matters escalated outside formal meetings?

Culture, Risk Culture and Remuneration

The role of boards and risk committees now explicitly include responsibility to maintain oversight of the culture, including risk culture, within an organisation.

A poor risk culture and immature risk management practices can result in excessive or ill-considered risk taking. This can, in turn, lead to financial losses, irreversible business decisions and reputation damage.

Directors should seek to ensure that:

- The tone from the top set by the board and management is consistent with the values of the organisation
- There is respect, compliance with and adherence to, the risk management frameworks, policies and procedures
- Risk issues are escalated in a timely and transparent manner
- Lessons are learned from risk incidents and issues
- There is alignment (and no misalignment) of the organisation's remuneration practice and policies and sound risk management

The theory and practice of risk culture continues to evolve. The Australian Prudential Regulation Authority's Final Report of the Prudential Inquiry into the Commonwealth Bank of Australia[5] released in May 2018 focused considerably on the importance of risk culture and the difficulties in establishing a sound risk culture.

The report highlighted that:

> "There is no single best practice for sound risk culture but there are, in principle, some common elements.
>
> They include a clear tone at the top and role modelling of good risk behaviours by leaders, constructive challenge from a range of perspectives, timely and transparent information flows without fear of blame, and a consistent approach to risk management …".

[5] https://www.apra.gov.au/sites/default/files/CBA-Prudential-Inquiry_Final-Report_30042018.pdf

The overall objective for the directors is to ensure that there are frameworks, governance arrangements, and risk and remuneration practices in place that appropriately balance risk and reward and assist the organisation operate in a sustainable manner in the long run.

Directors need to be alert to the risk of inappropriate, unethical, or unlawful behaviour in the organisation. Regular reporting of incidents, breaches and employee terminations is critical, including ensuring the effective working of whistle-blower arrangements. How directors manage serious risk incidents and breaches is also important to establishing a positive risk culture. This will be less about governance and more about exercising judgement.

Aligning an organisation's remuneration outcomes with its risk management goals and objectives is also an important role for directors. Key governance priorities and activities will include:

- Ensuring the performance plans and remuneration schemes for the executives have a strong and direct link to risk management outcomes
- Ensuring that the performance management frameworks across the organisation have meaningful risk management components
- Having agreed feedback mechanisms to communicate poor risk outcomes to the board and any human resources, people or remuneration committee that may be in place
- Being seen to make downward remuneration adjustments when there are significant risk issues

Questions to ask:

1. Does the board regularly assess and discuss risk culture?
2. Is there formal, regular reporting of employee risk and compliance incidents and breaches to the board?
3. Does the board take into account adverse risk outcomes into account when undertaking performance and remuneration reviews for executives?
4. Does the board understand the risk management components in the performance plans of all employees across the organisation?
5. Is there a formal process in place discuss lessons are learned from risk incidental and issues with management?

Diligent

a
MODERN
GOVERNANCE
company

Summary

This white paper seeks to provide directors with guidance on how to ensure that there is robust risk governance in place at the organisations they are involved in. Whilst many external events and risks are substantially out of their control, directors and management have full control over how they manage risk. This encompasses the design of the risk frameworks and governance, the frequently of reporting and discussions, and the level of investment in risk management capability.

About the Author

Peter Deans is a Non-Executive Director, and a former Chief Risk Officer. Peter is currently Chair and Non-Executive Director of Maia Financial Group (owned by KKR and HPS Investment Partners) and a Non-Executive Director of Trade for Good Pty Ltd and The Regtech Association.

Peter is a leading authority on risk management and the Creator & Founder of the 52 Risks® management framework.

About Diligent

Diligent is the pioneer in modern governance. Our trusted, cloud-based applications streamline the day-to-day work of board management and committees, support secure collaboration, manage subsidiary and entity data, and deliver insights that empower company leaders to make better decisions in today's complex landscape. With the largest global network of corporate directors and executives, Diligent is relied on by more than 19,000 organisations and nearly 700,000 leaders in over 90 countries. With award-winning customer service across the globe, Diligent serves more than 50% of the Fortune 1000, 70% of the FTSE 100 and 65% of the ASX.