Six Essential Steps in Establishing Sound Risk Governance and Management

*Mr. Peter Deans

Introduction

The board agenda is becoming more crowded with risk management issues. Is the world really a riskier place? How should our business think of the diverse range of social, political, environmental, and economic risks we face every day?

Directors and management alike are grappling with immediate issues in a post-COVID world whilst at the same time trying to develop longer-term strategies and growth options. Success in navigating this challenging world requires an insightful, efficient, and flexible approach to risk governance and risk management.

The article outlines six critical steps in establishing and maintaining sound risk governance and management. This will give an organisation the best chance of success in dealing with the risks - and opportunities - that are present both today and in the future.

A series of events since the commencement of the COVID pandemic in early 2020 has shaken boards and management teams like no other period in recent decades. Year-on-year revenue and profit growth were expected and rolled on. Ready access to equity, debt, and human capital was seen as the norm. Everything was freely available. New markets and customers were seemingly everywhere. During this period, the voice of risk management in many organisations was mostly silent and risk managers rarely talked to directors.

> It is important that directors and management agree on the desired risk culture across the organisation and how it will be built and periodically assessed.

The COVID pandemic and its knock-on effects – coupled with a range of other issues including climate change and geopolitical events and tensions – have woken up directors. The impact of these events has driven home the need for many organisations to reassess how they govern and manage risk. The benefits of having documented business continuity and crisis management practices are now well understood. Similarly, the benefits of having a risk management rhythm across an organisation to identify, assess, manage, and report on risks are now appreciated by many more boards.

What does good like, however? Where does an organisation start if it does not have the foundations of risk governance and oversight in place?

There are six key areas that a board and executive team should focus on to be able to effectively manage risk. They are as follows:

1. Board Level Commitment and Oversight
2. Documented Risk Management Framework (or Strategy)
3. Understanding the Risk Profile and Defining Risk Appetite
4. Risk Management Resourcing
5. Regular Risk Management Reporting
6. Establishing a Positive Risk Culture

Board Level Commitment and Oversight

The term 'the tone from the top' may seem an overused and worn-out management cliché. However, it is essential that the directors of a company or organisation demonstrate a commitment to managing risk in a structured and clearly communicated manner.

The most common method of doing this is by establishing a board subcommittee dedicated to overseeing risk management. Even small organisations can benefit from the establishment of a subcommittee. This committee can take one of many forms: a risk management committee, a risk and compliance committee, or a combined audit and risk committee. The establishment of this committee demonstrates to employees and external stakeholders – shareholders, investors, customers, suppliers, and the community - that the organisation is committed to managing risk. It is not just symbolic. Its existence increases the focus of the organisation on risk management through the various activities subsequently undertaken by and for the committee.

It is imperative that directors, the Chief Executive Officer (CEO) or Managing Director, and other business leaders frequently talk about the importance of managing risk and the risk characteristics of a high-performing organisation. This rhetoric also needs to be backed up by an ongoing investment in risk management. The importance of having dedicated risk management resources in place is covered later.

In all decision-making, the board and executive team also need to lead by example by asking questions about the risk implications of a decision, requesting risk assessments be undertaken, and seeking out specialist risk expertise for an independent view. This review and challenge are not about being risk-averse. It is ensuring that risk-taking is transparently assessed, measured, and understood.

Documented Risk Management Framework (or Strategy)

A foundational feature of sound risk governance and management is an overarching board-approved document that outlines how risk is governed and managed in the organisation. It should be a document that is shared with - and understood by - all personnel within the organisation including directors, the management team, and key employees with roles involving the management of risk.

The document often has different titles. It may be called a risk management framework, a risk management strategy, or a risk management policy. The name the document is given is not important. More important are its contents. It will contain both high-level statements about how the organisation manages risk and the types of risks it is willing to accept. A risk management framework will usually include:

- The governance approach to the management of risk across the organization, including an outline of the roles and responsibilities
- A list of key or material business risks for the organisation
- Statements about risk appetite for key or material risk categories (if not included in a separate document on risk appetite)
- The processes to be followed for risk identification; risk measurement and assessment and risk mitigation
- Organisational specific practices for risk monitoring, reporting, and escalation

It will be important that clarity around the organisational structure and specific roles and responsibilities is included in the risk management framework document.

Too often within an organisation, job descriptions or role summaries are outdated and don't include risk management areas of responsibility. In addition, internal documentation, operating manuals, and intranet pages may not have the latest business structure and an overview of who the key risk management contacts are. Keeping both updated can significantly improve the management of risk and risk outcomes.

Understanding the Risk Profile and Defining Risk Appetite

It is the board's role to agree on the nature and extent of the risks it is prepared to take to meet strategic and financial objectives. To achieve this, two key activities for directors are to (i) ensure that the organisation's key material business risks are identified and (ii) that appetite for risk-taking in these areas is defined and communicated.

The list of risks that directors and management need to consider and address can be daunting. For organisations that have not previously documented and assessed individual risks or built an enterprise-wide profile of their risks, it will take time to do this. Directors should ask management to prepare a list of material business risks in the first instance. This may involve the creation of risk hierarchies comprising major risk categories and subcategories.

The **52 Risks® framework** *(a free management framework that is documented at www.52Risks.com)* is a good starting point. It has common business risks grouped under strategic, financial, and operational risk categories. An organisation can then tailor its list of material risks by supplementing industry or business-specific risks. The final list of risk categories will assist directors and management discuss the risks using a common language.

It can be useful to incorporate into the risk management framework the requirement to formally update the risk profile of the organisation periodically. This can be undertaken half yearly or annually – depending on the size and nature of the organisation. An update can simply be a board memorandum from management providing their perspectives and views on the risks the organisation is facing. Alternatively, it can be a more comprehensive, bottom-up review of the existing, documented risks supplemented with a top-down overlay that considers a range of strategic risks and issues.

For organisations that choose to define risk appetite for their material business risks, the process will involve:

- Identifying the key material business risks
- Assessing and reviewing the likelihood and consequence of the risks occurring
- Agreeing on the appetite the organisation has for a specific risk or group of risks

For medium to large-sized organisations it is common to define risk appetite in a written, board-approved document referred to as a risk appetite statement. A risk appetite statement will document the material business risks to which the organisation is exposed, its appetite for each risk, and the approach to managing these risks.

It is important to assess both, the organisation's strategic plan and accompanying detailed business plans from a risk perspective. The strategic plan for the organisation and risk appetite set by the board needs to be aligned. In addition, as the external environment changes and a business changes or grows, it is important to regularly review risk appetite.

Risk Management Resourcing

The best-written and designed risk management frameworks and governance documents will sit on a shelf unless dedicated risk management personnel are in place, in even the smallest organisations.

It is important to identify a senior risk officer in the organisation and task them with bringing to life the management of risk. If there is not sufficient organisational breadth to appoint a dedicated senior person - such as a Chief Risk Officer (reporting to the Chief Executive Officer or Managing Director) - it is important to have a senior person in place at the next level below the C Suite. This role will usually be called the Head of Risk Management or Enterprise Risk Manager. The Chief Risk Officer (or the more junior role) will be responsible for:

- Overseeing and reporting on the operation of the risk management framework, strategy or policy
- Developing and periodically updating the enterprise risk profile of the organisation
- Assisting co-ordinate and report on risk management activities across the organisation managing specific sets of risks, such as workplace health and safety or cyber security
- Assisting with and/or undertaking periodic risk assessments across the organisation as required
- Preparing, submitting, and discussing risk management reports with the board and management

It is important for the board or risk management subcommittee to periodically satisfy itself that the risk management function is adequately resourced and undertaking the duties it has been tasked with. Inadequate risk management resources being committed will usually result in the organisation's risk management strategies and frameworks not being effectively implemented.

Regular Risk Management Reporting

Regular risk management to the board directly or via a subcommittee is vital to staying on top of risk management. Timely and insightful reporting of risk issues, near misses, changes in the risk profile of the organisation, emerging risks, and changes in the external environment will assist both board and management respond to both risks and opportunities.

The development and tracking of the organisation's performance against a set a of specific risk metrics, commonly

referred to as Key Risk Indicators (KRIs), will assist directors to monitor the organisation's adherence to the agreed risk appetite. These KRIs should be reported to the board regularly.

Experienced risk managers will ensure that directors are provided with the right level of data with appropriate insights. They will also avoid over-reporting. Lengthy reports lacking in insights will consume both valuable management time and time at board or subcommittee meetings.

Establishing a Positive Risk Culture

Defining, promoting, and periodically reviewing an organisation's risk culture is an activity that many directors and boards find challenging. It is worthwhile for directors to initially spend time with the management team and talking about risk culture. This goes hand in hand with the organisation's vision and values. It is important that directors and management agree on the desired risk culture across the organisation and how it will be built and periodically assessed.

The characteristics of organisations with a well-developed and mature approach to risk culture include:

- There is a defined organisational rhythm for communicating risk management objectives and priorities
- The objectives of the organisation's risk management frameworks, systems, and processes are well understood and articulated across the organisation
- Business owners are frequently observed proactively identifying, managing, and reporting risks
- Training programmes are in place for risk management education
- Risk management key performance indicators are included in performance plans and employee review processes
- Directors and management regularly review and discuss risk culture as a specific agenda item. For larger organisations, external reviews are often commissioned to review risk culture.

Conclusion

Boards and management teams can benefit from managing risks in a structured and disciplined manner. Putting in place sound foundational risk practices will assist them to quickly assess, respond to and manage the risks they face and also take advantage of opportunities. A small investment in getting better organised in governing and managing risk will pay off in the short-, medium-, and longer term.

Additional Resources:

1. North Carolina State University's ERM Initiative website has webinars, discussion papers, guides, and articles on enterprise risk management.
   https://erm.ncsu.edu/
2. The Governance Institute of Australia recently released a guide for directors.
   https://www.governanceinstitute.com.au/news-media/news/2022/jul/at-the-helm-in-uncertain-times-a-risk-management-guide-for-directors/
3. The 52 Risks website has a range of articles on risk management topics. The blog page is the best place to start.
   https://www.52risks.com/blog/

*__Mr. Peter Deans__ *is a Non-Executive Director, Risk Advisor, and former Chief Risk Officer. He is Creator & Founder of the 52 Risks® management framework, and a leading authority on risk management. Previously, he has been awarded Australian Banking & Finance magazine's Chief Risk Officer of the Year award in 2014, 2015, 2016, and 2018.*