Deloitte.

Risk Committee Resource Guide

For related information and guidance, visit the Deloitte Centre for Corporate Governance website at:

www.deloitte.co.za

Contents

Introduction

Risk committees become reality

This guide aims to assist board members of companies in designing, developing, and operating a board-level risk committee. In terms of the King Report of Governance for South Africa, 2009 (King III), it is recommended that the board should assign oversight of the company's risk management function to an appropriate board committee (for example a risk committee or the audit committee). This is in line with international developments, for example in the United States the Dodd-Frank Act requires such committees for certain bank holding companies.

Deloitte developed this guide in response to growing interest in board-level risk committees. While many companies already have a risk committee (or in many instances a combined audit and risk committee), quite a few do not. Also, companies that do have risk committees may benefit from revisiting their risk committee charters and activities. In doing so, the board can ascertain that the risk committee has the composition, reporting relationships, and responsibilities that best suit the enterprise.

This resource guide first presents considerations for a board contemplating the formation of a risk committee (Section 1). It then covers topics that a risk committee charter might include, as well as guidance on developing and using the charter (Section 2). Next, the guide provides suggestions related to how a risk committee may go about fulfilling its chief responsibilities (Section 3), and overview of the Risk Intelligent approach to risk management (Section 4) and educating and evaluating itself (Section 5). Most sections include example related questions to ask when developing a risk committee.

While risk management is not a new concept, many companies are refreshing their thinking with regard to risk governance and oversight as disciplines for many board members. We trust that this guide will help improve board members' and senior executives' knowledge of risk committees and of risk governance and oversight. We encourage interested readers to make use of the tools and resources mentioned and included in the appendix of this guide.

[1]The Dodd-Frank Wall Street Reform and Consumer Protection Act is a federal statute in the United States signed into law by President Barack Obama on July 21, 2010. It promotes the financial stability of the United States by improving accountability and transparency in the financial system, ending "too big to fail," protecting the American taxpayer by ending bailouts, protecting consumers from abusive financial services practices, and other purposes.

Components of risk management

Section 1

Considerations in forming a risk committee

According to King III the board is responsible for the governance of risk through formal processes, which include the total system and process of risk management. The board should show leadership in guiding the efforts aimed at meeting risk management expectations and requirements. Although the board remains ultimately responsible for the governance of risk, it may delegate this function to a separate committee.

The Listings Requirements of the Johannesburg Stock Exchange (JSE) require listed companies to have a risk committee comprising a minimum of three members. Membership of the risk committee should include executive and non-executive directors. Those members of senior management responsible for the various areas of risk management should attend the meetings. The chairman of the board may be a member of this committee but must not chair it.

The role of the committee is to perform an oversight function. In doing so, it should consider the risk policy and plan, determine the company's risk appetite and risk tolerance, ensure that risk assessments are performed regularly, and ensure that the company has and maintains an effective on-going risk assessment process, consisting of risk identification, risk quantification and risk evaluation. This risk assessment process (using a generally recognised methodology) should identify risks and opportunities, and measure their potential impact and likelihood. The committee should receive assurance from internal and external assurance providers regarding the effectiveness of the risk management process. In turn, management is responsible for the design, implementation and effectiveness of risk management, as well as continual risk monitoring.

It is of vital importance that members of the risk committee have experience within the industry. This would allow them to identify areas of risk and be aware of the appropriate methods of managing the company's exposure via internal (the control environment) or external (such as thorough insurance cover) means.

Risk management is an often misunderstood discipline within a company. Too often the responsibility for ensuring that the significant risks identified and adequately managed is not acknowledged, or is inappropriately delegated to the audit committee. There are two reasons why the risk management function should not report to the audit committee, but should be monitored by a separate risk committee. The first is that, as a consequence of the prescribed composition of the audit committee (all members must be independent non-executive directors), the function will often have financial focus when risk management should correctly extend far beyond the finances of a company.

Secondly, the audit committee should act as an independent oversight body. Having to directly oversee the risk management function would generally involve a large amount of detailed review of the processes and workings of the company. This would necessarily have a detrimental effect on the objectivity of the audit committee's members when considering reports of the risk management function. The formation of a separate committee recognises the fact that the identification and management of risks impacting the business, and the disclosure of these to the shareholders is vital to good governance.

In addition, the JSE is aware that some listed companies combine the audit and risk committee. The JSE warns that, given the difference in the membership of these committees, listed companies must ensure that in these instances that the membership of the combined committee meets the more stringent independence criteria of the audit committee as set out in the Companies Act and King III. The result of a combined committee is that all the members must be independent non-executive directors. This precludes executive directors (such as the CEO and CFO) from membership. However, given the key role of the CEO in the risk management process, best practice (as captured in King III) requires the risk committee to comprise a combination of executive and non-executive directors.

Also, a combined audit and risk committee will inevitably have a strong focus on financial risks, which may result in inadequate attention to operation and related risk.

It is our recommendation that the responsibility for risk management be delegated by the board to a separate risk committee, comprising both executive and non-executive directors. Where more than one committee bears responsibility for risk management (i.e. the audit committee oversees financial risks and the remuneration committee oversees risks pertaining to compensation), it is paramount that the responsibilities are clearly demarcated and that communication channels are established to ensure that the respective committees take cognisance of and consider the reports and recommendations of the other relevant committees.

In considering whether or not to establish a risk committee one might consider the following key factors:

- *Inherent risk environment:* The need for a risk committee may be precipitated by the inherent risk environment. The extent, complexity, and potential impact of risks should be considered, and weighed against the ability of the board or a board committee (e.g. the audit committee) to deal sufficiently with workload.

- *The needs of stakeholders:* The needs of the enterprise and its stakeholders should be considered. It may also behove the board to assess the quality and comprehensiveness of the current risk governance and oversight structure, the risk environment, and the future needs of the organisation. The composition and activities of the risk committee and its relationship with other board committees could reflect the board's assessment of those factors.
- *Alignment of risk governance with strategy*: The board should consider whether risk oversight and management are aligned with management's strategy. Enterprises vary widely in their business models, risk appetite, and approaches to risk management. A key consideration is that the board, management, and business units be aligned in their approach to risk and strategy - to promote risk-taking for reward in the context of sound risk governance.
- *Oversight of the risk management infrastructure:* A question to consider is whether the risk committee is responsible for overseeing the risk management infrastructure - the people, processes, and resources of the risk management program - or whether the audit committee or entire board will oversee it.
- *Scope of risk committee responsibilities:* The board may need to decide whether the risk committee will be responsible for overseeing all risks, or whether other committees, such as the audit committee or the remuneration committee, will be responsible for some. For example, oversight of risks associated with financial reporting may remain under the audit committee, while those associated with executive remuneration plans might remain with the remuneration committee. But because functional risks (such as tax or human resources risk) are often connected to operational or strategic risks, it is important to consider how the interconnectivity of risks is addressed. In any event, the board will need to determine which committees will oversee which risks.
- *Communication among committees:* The board should consider how the committees will keep one another - and the board itself - informed about risks and risk-oversight practices. Efficiency and effectiveness call for clear boundaries, communication channels, and handoff points. This need may require the board to define these elements clearly, making adjustments as needed.

General role of the risk committee

The risk committee will have specific responsibilities that include, but are not limited to, oversight and approval of the enterprise risk management framework commensurate with the complexity of the company including (note that these responsibilities are performed by the committee on behalf of the board – ultimately the board remains responsible for the final approval of the risk policy and risk management):

- Oversight of risk appetite and risk tolerance appropriate to each business line of the company
- Appropriate policies and procedures relating to risk management governance, risk management practices, and risk control infrastructure for the enterprise as a whole
- Processes and systems for identifying and reporting risks and risk-management deficiencies, including emerging risks, on an enterprise-wide basis
- Monitoring of compliance with the company's risk limit structure and policies and procedures relating to risk management governance, practices, and risk controls across the enterprise
- Effective and timely implementation of corrective actions to address risk management deficiencies
- Specification of management and employees' authority and independence to carry out risk management responsibilities, and
- Integration of risk management and control objectives in management goals and the company's compensation structure.

The risk governance infrastructure

The totality of the risk governance infrastructure includes the oversight provided by board committees in their risk-related roles. The risk governance infrastructure sets forth how the board defines the role of board committees and the full board in overseeing risk. For example, is there a separate risk committee of the board or is risk oversight handled only by the audit committee or spread across committees, depending on expertise? And, finally, what is the role of the full board in overseeing risk?

To establish an appropriate risk governance infrastructure, the board might consider defining the risk-related roles and responsibilities of each committee as well as clear boundaries and communication channels among them. The board will need to understand and define which committees are responsible for which risks and how each committee oversees risks.

Sample questions to ask about forming a risk committee:

- How long is the term of service for members and for the chair? Will the chair position rotate, or will he/she be appointed or reappointed by vote or other means?
- What are the responsibilities of the risk committee and of the committee chair?
- How will the chair, the committee, and its members be evaluated?
- Will the management risk committee report to the risk committee, the Chief Risk Officer (CRO), or the CEO? Are subsidiaries or other related entities subject to the risk committee?
- Which risks will the risk committee oversee and which will be left to other board committees?
- Which board members have the experience to be on the risk committee, and how can the company attract and cultivate appropriate risk committee members?
- How will the board keep abreast of changes in regulations and in risk governance and management practices?
- How will the board ensure that the committee has access to the people and resources it will need to carry out its responsibilities?

Risk committee charter and composition

Risk committee charter

Often, the board and its risk committee define their roles in risk oversight and governance by means of the risk committee charter. The charter is also among the main tools the board has for disclosing its approach to risk oversight. In writing the charter, the board and the risk committee will determine the risk committee's role and responsibilities in risk governance.

Board committee charters specify the committee's responsibilities and how it carries them out. The risk committee charter discloses the board's involvement in and approach to risk oversight, the committee's relationship to the CEO, Chief Risk Office (CRO) and to management's risk committee, and other key elements of risk oversight.

In developing risk committee charters, boards may wish to consider including provisions that specifies:

- The separate nature of the risk committee and that it has been established to exercise enterprise-wide risk-oversight responsibilities
- The risk-oversight responsibilities of the committee and how it fulfils them
- Who is responsible for oversight of management's risk committee, for example, whether it is the CRO, the risk committee, the full board, or the CEO (although, typically, the full board is ultimately accountable and responsible for risk governance)
- Who is responsible for establishing the criteria for management's reporting about risk to the board (although the actual criteria need not be set in the charter, because they are expected to change as the enterprise and risks change)
- The composition of the risk committee and the qualifications of risk committee members
- The board's or risk committee's responsibilities regarding the enterprise's risk appetite, risk tolerances, and utilisation of the risk appetite
- The board's or risk committee's responsibility to oversee risk exposures and risk strategy for broadly defined risks, including for example credit, market, operational, compliance, legal, property, security, IT, and reputational risks

- The risk committee's responsibility to oversee the identification, assessment, and monitoring of risk on an on-going enterprise-wide and individual-entity or line of business basis
- The risk committee's responsibility to approve the charter of the management risk committee - if the board, in compliance with the company's Memorandum of Incorporation, delegates that responsibility to the risk committee
- The reporting relationships between the risk committee, the CEO, the CRO and the management risk committee
- The risk committee's oversight of management's implementation of the risk management strategy
- The risk committee's responsibility to ensure that risk management is embedded in the business and all decision making processes
- The use of specialist in areas where risks are complex
- Terms of service of risk committee members and the chair, with incumbents subject to reappointment; term limits (which may preclude members or chairs from having their terms renewed) may not be desirable because they may cause the loss of individuals in valued roles

In general, the more precise the charter, the better positioned the risk committee will be to exercise oversight. For example, a detailed charter should enable the committee to develop an annual meeting calendar, based on the responsibilities and required meeting frequency. The calendar might include, for example, specific risk issues (such as risk appetite) and activities (such as risk committee education) for discussion, as well as meeting agendas, using the responsibilities in the charter as a guide.

In addition, it may be appropriate to coordinate the risk committee calendar with those of the audit, remuneration, and nominations committees so that the risk committee will, at a minimum, be made aware of the risk-related activities of those committees. Coordinating their calendars enables the committees to coordinate their activities and use of resources to maximise risk-oversight efficiency.

Tools and resources. Deloitte has developed a model risk committee charter as a guide and template for boards and committees that are developing their charters. The model risk committee charter is located in Appendix A and can be used with the calendar planning tool in Appendix B.

Developing and using the risk committee charter

The following guidelines can be considered by a board or risk committee as they develop and use a risk committee charter:

- *Develop the charter as a group:* Risk committee members, under the guidance and with the approval of the full board, could develop the charter as a group (perhaps with the assistance of an external facilitator). While the actual writing of the charter can be delegated to management, input from the board and committee members should be considered regarding the key principles embedded in the charter, which risks will be overseen, whether the CEO/CRO will report to the risk committee, and other key points. Ideally, all risk committee members would agree to the charter and approve it - as would the board.
- *Use the charter as a guide:* A risk charter is not to be written and shelved but instead put to use. When the committee is in doubt as to its responsibilities, or feels the need to assert its risk governance role with senior executives, it can reference the charter for guidance. Providing the charter as part of the orientation package for new members of the board and its committees may help on-boarding and may be used in locating and hiring the committee's members, who may be recruited from among existing board members or elsewhere.
- *Review the charter annually:* An annual review of the charter to update the committee's role in risk oversight by the board and risk committee may also be required. The charter should be updated as needed to keep the committee's structure and practices in line with regulatory requirements and the enterprise's needs. It could also be periodically reviewed by a qualified external third party to assess whether the committee's structure and responsibilities reflect leading practices in the industry. The results of a regular review of the effectiveness of the committee may also provide useful guidance with respect to the content of the charter.

Composition of the risk committee

The Companies Act provides the board with the power to appoint board committees, and to delegate to such committees any of the authority of the board. The authority of the board to appoint board committees is subject to the company's Memorandum of Incorporation. If the company's Memorandum of Incorporation, or a board resolution establishing a committee, does not provide otherwise, the committee may include persons who are not directors of the company. However, it should be noted that where non-directors are appointed to a board committee, such persons are not allowed to vote on a matter to be decided by the committee

Board committees constitute an important element of the governance process and should be established with clearly agreed reporting procedures and a written scope of authority. The Act recognises the right of a board to establish board committees but by doing so, the board is not exonerated of complying with its legal responsibilities.
- King III principle 2.23 par 125

Consider having risk committee members who are knowledgeable about risk governance and management and about the risks the enterprise faces and methods of managing them. It may be advantageous to have risk committee members with knowledge of business activities, processes, and risks appropriate to the size and scope of the enterprise, as well as the time, energy, and willingness to serve as active contributors.

The composition of the risk committee (as proposed by King III) is somewhat unique in that it should comprise a combination of directors (both executive and non-executive directors) and non-directors. The JSE (through the application of King III) echoes the requirement that both executive and non-executive directors be appointed to the committee. (King III indicates that all other committees should comprise only non-executive directors, of which the majority should be independent). Neither King III nor the JSE requires the appointment of independent directors on the risk committee. The chairman of the board may me a member of this committee but must not chair it.

Members of the risk committee, taken as a whole, should comprise people with adequate risk management skills and experience to equip the committee to perform its functions. To supplement its risk management skills and experience, the risk committee may invite independent risk management experts to attend its meetings.

Those members of senior management responsible for the various areas of risk management should attend its meetings.

As with all matters related to board composition, the nominations committee typically has the authority to define the qualifications of its members. It can also help determine whether current board members can provide the needed skills. In most organisations, the nominations committee would assist in recruiting, vetting, and approving risk committee members.

Risk committee members may be recruited from the current board and should ideally include a combination of executive and non-executive directors.

As there is some overlap between the functions of the audit committee (responsible for among others overseeing the management of financial risks) and the risk committee (responsible for all other risks), we find that there is often an overlap in membership of the audit committee and the risk committee. Many companies find it appropriate to appoint one or two members of the audit committee, one or two other non-executive directors, as well as the CEO and the CFO as members of the risk committee. Of course, the collective membership of the committee should account for the range of skill and experience required to guide management and perform effective oversight with respect to the risk management process. Other relevant members of the senior management team (for example the Chief Internal Auditor, Chief Risk Officer, Chief Information Officer, etc.) are invited to attend all meetings.

Asking questions and considerations related to the composition of the risk committee is one element of effective board succession and development plans.

Notes:

Fulfilling risk-oversight responsibilities

Successful risk oversight depends, in part, on the ways in which the risk committee fulfils its responsibilities and interacts with the executive team, CRO, board, and stakeholders.

Responsibilities

Broadly, the responsibilities of a risk committee may include the following:

- **Oversee the risk management infrastructure:** The full board may oversee the organisation's risk management infrastructure (see sidebar below), or this oversight responsibility can be delegated to the risk committee, rather than to the audit committee (the committee that historically has had primary responsibility for overseeing the risk management infrastructure). The JSE Listing Requirements permit the board of a listed company to delegate this responsibility to a risk committee, rather than to the audit committee – where the responsibility is delegated to a combined audit and risk committee, listed companies must ensure that in these instances the membership of the combined committee meets the more stringent independence criteria of the audit committee as set out in King III (see comments above).
- **Address risk and strategy simultaneously:** Address risk management and governance when strategies for growth and value creation are being created and management decisions are being made. The purpose of this responsibility is typically not to promote risk avoidance, but the opposite - to promote risk-taking for reward in the context of sound risk governance.

- **Approve the risk management policy and plan:** The risk committee should be able to demonstrate that it has dealt with the governance of risk comprehensively. This should include the development and implementation of a policy and plan for a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, as well as the related internal control, compliance and governance processes within the company. Management should develop both the risk management policy and the plan for approval by the committee. The risk management policy should set the tone for risk management in the company and should indicate how risk management will support the company's strategy. The risk management policy should include the company's definitions of risk and risk management, the risk management objectives, the risk approach and philosophy, as well as the various responsibilities and ownership for risk management within the company. The risk management plan should consider the maturity of the risk management of the company and should be tailored to the specific circumstances of the company. The risk management plan should include:
  - the company's risk management structure
  - the risk management framework i.e. the approach followed, for instance, COSO, ISO, IRMSA ERM Code of Practice, etc.
  - the standards and methodology adopted – this refers to the measureable milestones such as tolerances, intervals, frequencies, frequency rates, etc.
  - risk management guidelines
  - reference to integration through, for instance, training and awareness programmes, and
  - details of the assurance and review of the risk management process.

  The committee should review its risk management plan regularly but at least once a year.
- **Approve the process for risk identification:** The risk management plan should set out the process for risk identification. This can take various forms, e.g. scenario planning, a management workshop, etc. The risk committee should assess the robustness of the process for the identification of all risks, and review and approve outcomes of the process.

- **Assist with risk appetite and tolerance:** The risk committee should help establish, communicate, and monitor the risk culture, risk appetite, risk tolerances, and risk utilisation of the organisation at the enterprise and business-unit levels. Risk appetite defines the level of enterprise-wide risk that leaders are willing to take (or not take) with respect to specific actions, such as acquisitions, new product development, or market expansion. Where quantification is practical, risk appetite is usually expressed as a monetary figure or as a percentage of revenue, capital, or other financial measure (such as loan losses); however, we recommend that less quantifiable risk areas, such as reputational risk, also be considered when setting risk appetite levels. Once the risk appetite is defined, the committee (in consultation with management) then should define specific risk tolerances, also known as risk targets or limits, that express the specific threshold level of risk by incident in terms that decision-makers can use (for instance, in completing an acquisition, the risk tolerance may be defined as a stop-loss threshold of a specified value).
- **Monitor risks:** The committee should assist in assessing and monitoring the company's compliance with the risk limit structure and effective remediation of non-compliance on an on-going, enterprise-wide, and individual-entity basis. For the risk committee, this responsibility extends to all risks, or at least to all risks not monitored by the audit, remuneration, or other board-level committees. In cases of risks monitored by other board committees, the risk committee should be made aware of on-going risks.
- **Oversee risk exposures:** It's important that the risk committee develop a view into critical risks and exposures and into management's strategy for addressing them. The committee should consider the full range of risks and potential interactions among risks, including risk concentrations, escalating and de-escalating risks, contingent risks, and inherent and residual risk.

- **Correlate risks:** The committee should assist the board to ensure that the board is satisfied that insurance, indemnification and remuneration practices do not prejudice risk management decision-making.
- **Advise the board on risk strategy:** The board creates the risk committee to serve as a repository of information and expertise on risk and to advise the board on risk strategy. Thus, the risk committee can help inform the board of risk exposures and advise the board on future risk strategy. In this regard, it should be noted that King III proposes that risk management should be intrusive: its methodology and techniques should be embedded within strategy setting, planning, and business processes to safeguard performance and sustainability. The rigours of risk management should provide responses and interventions that strive to create an appropriate balance between risk and reward within the company.

In line with the Risk Intelligent approach to risk management (see section 4), it is important that the risk committee assist management to ensure the incorporation of Risk Intelligence into the strategy of the business. In this regard, the risk committee should guide the design of processes for integrating risk management into strategic planning, to continuously monitor strategic alignment of risk management and establish accountability by reinforcing executive accountability for risk management.

Steps some boards have taken to improve risk governance:

- Revised committee charters to include risk-related concerns
- Benchmarked their practices against peer companies
- Obtained guidance from associations of directors and similar sources
- Focused more attention on risk management and its value and shortcomings
- Reviewed ethical guidelines and codes of conduct

- **Foster an appropriate risk culture:** The committee should work towards embedding a risk culture where people at every level manage risk as an intrinsic part of their jobs. Rather than being risk averse, they should understand the risks of any activity they undertake and manage them accordingly. Such a culture supports open discussion about uncertainties, encourages employees to express concerns, and maintains processes to elevate concerns to appropriate levels.
- **Approve management risk committee charters:** Management may establish risk committees not only at the enterprise level, but also in some cases at business-unit levels. The risk committee should consider and approve the charters of any such management risk committees.
- **Central role of the CEO:** It should be noted that King III stresses that although a CRO may be appointed to assist the CEO with the execution of the risk management process, the accountability to the board remains with the CEO. There should however be an appreciation that execution of risk management does not reside in one individual but requires an inclusive team-based approach for effective application across the company.

Questions to consider regarding a Chief Risk Officer:

- What specific qualifications does the CEO seek in the CRO?
- Has this person served as a CEO, CRO, CFO, or CCO, or in another position with substantial risk-related responsibilities? How recent is his or her experience?
- What was the industry, size, and scope of the organisation(s) and which risks did he or she manage or oversee? How do the businesses and risks that the individual previously oversaw compare with those of the company?
- What was the nature of regulatory requirements and expectations for risk management in the individual's prior organisation?
- How hands on and in depth is his or her experience? In other words, did he or she just sign-off on risk management or oversight reports or was he or she truly involved?
- What was the size of the risk organisation and what role did the individual play in developing and overseeing the risk organisation?
- What were the results of risk management and governance activities during and after this person's watch? What were his or her successes and failures and how does he or she view them?
- How risk averse or risk tolerant is this person in organisational settings?
- Has this individual had the experience of identifying, analysing, monitoring, and reporting on risk to a board?
- Is this individual a good fit with the executive team and the board in terms of personality, team orientation, communication skills, and leadership style?

- **Consult external experts:** The risk committee should consider having access to external expert advice regarding risk and risk governance and management in the form of meetings, presentations, verbal or written briefings, or assignments commissioned by the risk committee. Areas to cover could include the risk environment, regulatory developments, leading practices, or any other items the board or committee specifies. In some cases, the risk committee may seek external board education regarding risk management or regulatory matters. In other cases, the risk committee may engage a consultant for a particular assessment or other efforts best commissioned at the board level.
- **IT governance:** King III makes it clear that the board must ensure proper governance of information technology (IT) risk, including information security. As such, IT risks form an integral part of company's risk management processes. The risk committee may be assigned responsibility to oversee IT risk management. In this regard, the role of the risk committee is to ensure proper alignment of IT with the strategy, performance and sustainability objectives of the company, the implementation of an IT governance framework, oversight of the management of information assets, and monitoring and evaluation of all significant investments and expenditure in IT.
- **Consider other responsibilities:** Depending on the enterprise, its industry, and its approach to value creation, the risk committee may want to involve itself in other responsibilities. The work of the risk committee can help its members to be better positioned to add value within the board and the organisation.

The board and/or the risk committee can assert its responsibilities in any given area by writing them into the risk committee charter.

The risk management infrastructure

An organisation's risk management infrastructure includes the people, processes, and technology required to identify measure, monitor, mitigate, and manage the risks the enterprise faces. An infrastructure with these components can help provide management with information to help assess and manage risk.

The risk committee should review the risk infrastructure. If an adequate infrastructure is not in place, management must consider whether to scale back its risk-taking to appropriate levels or scale up the infrastructure to adequate levels or take other agreed-upon action.

Overseers of risk may rely on the risk management infrastructure for the information required to exercise proper oversight. Thus, potential indicators of an inadequate infrastructure can be the lack of adequate and timely information about risk, inconclusive discussions about risk, or feelings of being uninformed about risks. This may or may not indicate a need for a risk committee, but it could point to the need for improved information to support risk.

At the action level

In addition to the above responsibilities, the risk committee might also consider the following:

- **Locate gaps and overlaps**: Given its enterprise-wide view of risk, the risk committee is positioned to locate gaps and points of overlap between board committees. If any are discovered, the committee may be positioned to recommend ways to address them and define or redefine appropriate boundaries and communication channels.
- **Require risk reporting to the board:** The committee should consider how to define significant decisions, transactions, positions, and other items that management should bring to the risk committee's and board's attention. These may be defined by type, transaction size, amount of exposure, and any other criteria the board or risk committee specifies.
- **Provide adequate funding:** The risk committee can also influence the adequacy of budgets and resources for risk governance and management which are appropriate.
- **Recognise IT's role:** IT is integral to risk management and oversight in every organisation. Given this fact, the risk committee must understand the role of IT in the risk management infrastructure and the risks to IT as well as those posed by cybercrime and other cyber threats.

- **Review crisis management plans:** Keep abreast of crisis preparedness and ascertain that management has developed and can implement a plan to respond to major risks, such as natural disasters, terrorism, cyber-attacks, epidemics, civil disorder, black swan events, and other events that could compromise the enterprise's human or other resources or disrupt the value chain.

Focus on correlated risk

Interdependencies among risks often cross business-unit and functional boundaries. Attempts to mitigate risk in one area, such as operations, may affect risk exposure in other areas, such as finance, tax, IT, or human resources, and vice versa. Or different areas of the business may independently pursue rewarded risk activities that, while remaining within each group's individual risk tolerance, create unacceptable risks for the company as a whole. Sometimes, organisational silos can mask important connections even in closely related areas such as liquidity and credit risk which may be managed in different parts of the organisation.

To illustrate, consider supply chain risk. Examining supply chain risk as an operational risk might fail to account for dependent risks that are often managed in silos, such as activities related to transfer pricing, the US Foreign Corrupt Practices Act, supplier issues, legal versus beneficial ownership of intangible assets overseas, value-added tax, customs and licensing, currency issues, global regulatory compliance, or deployment of staff overseas. A risk event in any of these areas can create a ripple effect through the others, leading to unintended consequences. Examples include: results of a significant transfer-pricing decision could wipe out the economic benefit of an otherwise rational and tax-efficient supply chain strategy. Sanctions from a foreign government could put a valuable link in the supply chain in jeopardy. Failing to appreciate the legal environment in a geography might result in the loss of a valuable patent to nationalisation, one upon which key manufacturing processes depend. Lack of preparation in the implementation or maintenance phases throughout an organisation's supply chain management cycle may result in an unanticipated tax burden associated with exit charges and/or permanent establishment risk.

If these risks are examined individually but not considered together as companies assess their supply chain strategy, the extent of the upside and downside risk in the supply chain cannot be fully appreciated. Excluding any one of these could lead to a business decision that doesn't contemplate risk holistically across the organisation. Mitigation in one area could increase the significance of the risk in the other, or failing to aggregate the risk could mean that mitigation is postponed inappropriately.

Risk-oversight disclosures

King III requires the board to disclose in the company's Integrated Report how it has satisfied itself that risk assessments, responses and interventions are effective. In order to provide a comprehensive report to shareholders and other stakeholders, Deloitte has developed a list of points which boards, risk committees, and senior management can use to help determine what may be appropriate and useful to disclose:

- Whether the full board is responsible for risk
- Whether the company has a separate risk committee
- Whether the risk committee or the audit committee is the primary committee responsible for risk
- Whether other board committees are involved in risk oversight
- Whether the remuneration committee is responsible for overseeing risk in remuneration plans
- Whether the CEO is responsible for risk management or how the CEO is involved in risk
- Whether the company has a CRO
- The board's involvement with regard to the company's risk appetite
- How the board is involved with regard to corporate culture
- Whether risk oversight and management are aligned with the company's strategy
- Whether the company has a risk committee at the management level
- Whether the company separately addresses reputational risk
- Whether any undue, unexpected or unusual risks were taken in the pursuit of reward as well as any material losses and the causes of the losses. This disclosure should be made with due regard to the company's commercially privileged information. In disclosing the material losses, the board should endeavour to quantify and disclose the impact that these losses have on the company and the responses and interventions implemented by the board and management to prevent recurrence of the losses.

Identification of key risks and opportunities, and linking this to materiality in the Integrated Report

With the release of the Integrated Reporting Framework, the International Integrated Reporting Council has provided further guidance to companies on what principles and content elements should be adopted when preparing an Integrated Report.

Consequently there are two areas that the risk committee should be aware of and over time may become responsible for. These include the materiality determination process and the reporting of risk and opportunities.

In determining whether or not a matter is material, senior management and the board consider whether the matter substantively impacts, or has the potential to substantively impact, the organisation's strategy, its business model, or one or more of the capitals it uses or affects. The principle here is that, if the board needs certain information to take key strategic decisions, this point to the materiality of the information.

As such, the board agenda and board pack may provide a very clear indication of what information is regarded as material by the board. Of course, this approach to materiality necessitates greater alignment between material matter identification and assessment and the risk management process.

In disclosing the key risks and opportunities in the Integrated Report, the risk committee should provide the oversight over this element of disclosure in the Integrate Report prior to board approval. The disclosure point should influence the risk committee's in year reporting and focus on not only the downside but the upside of risk management.

Overview of risk and of management's risk management responsibilities

- How do we define risk appetite and risk tolerance, at both the enterprise and business-unit levels?
- How do we measure the risk utilisation and exposures of the organisation at the enterprise and business-unit levels?
- What are the components of the risk management infrastructure and how do we know they are adequate to address the risks the enterprise faces?
- Have the audit committee and remuneration committee gauged the risks that they oversee in financial reports and remuneration systems and reported them to the risk committee?
- Are we receiving the information from management that we have requested and has it been timely?
- Have we used the risk-related information from the CEO, CRO and management to monitor the risk appetite and risk profile, and in a timely manner?
- Do we review and concur with the organisation's disclosures regarding risks in the Integrated Report and other public documents before they are issued?

Notes:

Section 4

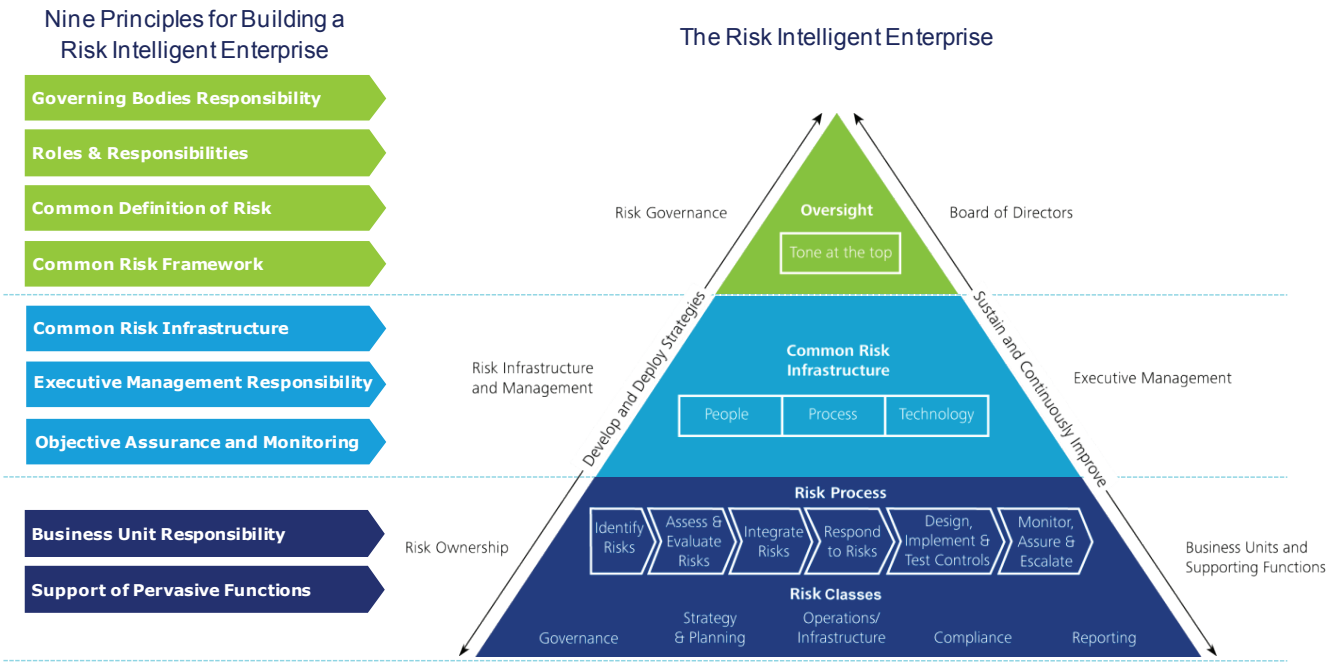
Risk intelligent enterprise

At many organisations, risk governance and value creation are viewed as opposed or even as mutually exclusive, when in fact they are inseparable. Every decision, activity, and initiative that aims to create or protect value involves some degree of risk. Hence, effective risk governance calls for Risk Intelligent governance - an approach that seeks not to discourage appropriate risk-taking, but to embed appropriate risk management procedures into all of an enterprise's business pursuits.

Deloitte's concept of the Risk Intelligent Enterprise integrates nine principles related to the responsibilities of the board, senior management, and business unit leaders into a cohesive risk management framework. Risk governance is at the apex of the framework: the unifying touchstone and guide to all of the organisation's risk management efforts. But on a more detailed level, what does effective Risk Intelligent governance entail?

Nine fundamental principles of a Risk Intelligence program

1. In a Risk Intelligent Enterprise, a common definition of risk, which addresses both value preservation and value creation, is used consistently throughout the organisation.
2. In a Risk Intelligent Enterprise, a common risk framework supported by appropriate standards is used throughout the organisation to manage risks.
3. In a Risk Intelligent Enterprise, key roles, responsibilities, and authority relating to risk management are clearly defined and delineated within the organisation.
4. In a Risk Intelligent Enterprise, a common risk management infrastructure is used to support the business units and functions in the performance of their risk responsibilities.
5. In a Risk Intelligent Enterprise, governing bodies (e.g., boards, risk committees, audit committees, etc.) have appropriate transparency and visibility into the organisation's risk management practices to discharge their responsibilities.
6. In a Risk Intelligent Enterprise, executive management is charged with primary responsibility for designing, implementing, and maintaining an effective risk program.
7. In a Risk Intelligent Enterprise, business units (departments, agencies, etc.) are responsible for the performance of their business and the management of risks they take within the risk framework established by executive management.
8. In a Risk Intelligent Enterprise, certain functions (e.g., Finance, Legal, Tax, IT, HR, etc.) have a pervasive impact on the business and provide support to the business units as it relates to the organisation's risk program.
9. In a Risk Intelligent Enterprise, certain functions (e.g., internal audit, risk management, compliance, etc.) provide objective assurance as well as monitor and report on the effectiveness of an organisation's risk program to governing bodies and executive management.



Based on our experience working with boards in their risk governance efforts, we have identified six distinct actions a board can take to help enable a Risk Intelligent governance approach:

1. Define the board's risk oversight role (delegated to the risk committee)
2. Foster a Risk Intelligent culture
3. Help management incorporate Risk Intelligence into strategy
4. Help define the risk appetite
5. Execute the Risk Intelligent governance process
6. Benchmark and evaluate the governance process

Collectively, these "areas of focus" reflect the view that risk-taking for reward and growth is as important as risk mitigation to protect existing assets. By treating risk as intrinsic to the conduct of business, Risk Intelligent governance elevates risk management from an exercise in risk avoidance to an essential consideration in every decision, activity, and initiative.

Area of focus 1: Define the board's risk oversight role

Effective risk oversight begins with a solid mutual understanding of the extent and nature of the board's responsibilities as compared to those of management and other stakeholders. Key board-level responsibilities include setting the expectations and tone, elevating risk as a priority, and initiating the communication and activities that constitute intelligent risk management. The ultimate goal is to assist management in creating a cohesive process in which risks and their impacts are routinely identified, evaluated, and addressed.

A board should possess enough collective knowledge and experience to promote a broad perspective, open dialogue, and useful insights regarding risk.

Actions to consider in defining the board's risk oversight role:

- *Define the board's risk governance roles and responsibilities.* Although the entire board is accountable for overseeing risk management and should be involved in the risk oversight process, it may delegate responsibility for risk oversight to the risk committee. Having various committees play complementary roles in risk oversight (e.g. risk committee, audit committee, remuneration committee, etc.) - and share their findings and insights with each other and the entire board - can help set the tone that risk oversight is important to all board and committee members. Even in boards where the nominal responsibility for risk oversight rests with a single committee all board members should recognise that risk oversight is broader than that single committee. In any case, all such roles and responsibilities should be formally defined and clearly understood.

- *Consider board composition.* In our view, a board should possess enough collective knowledge and experience to promote a broad perspective, open dialogue, and useful insights regarding risk. Consider performing a periodic evaluation, perhaps carried out by the nominations committee, of the board's overall composition as well as each member's experiences, knowledge, and special characteristics and qualities. Having the right mix of board members at the table will allow for discussions that are founded on Risk Intelligent knowledge and perspective.
- *Establish an enterprise-wide risk management framework.* Like any organisational process, risk management requires a framework that defines its goals, roles, activities, and desired results. Deloitte's concept of the Risk Intelligent Enterprise describes an approach to risk that can strengthen an existing framework or constitute a framework itself. Ideally, the chosen framework will help management establish goals, terms, methods, and measures, as well as gauge the need for specific programs (such as a contract risk and compliance program or training programs on risk awareness).
- *Perform site visits.* Consider touring the organisation's facilities to enhance your understanding of work processes and the risks associated with value creation and preservation. A number of boards today are indeed using site visits to broaden their knowledge of - and demonstrate their interest in – the work of the enterprise.

Questions to ask about risk oversight:

- How is risk overseen by our various board committees?
- Is there appropriate coordination and communication?
- Are we getting the information and insights we need for key decisions?
- Which framework has management selected for the risk management program? What criteria did they use to select it?
- What mechanisms does management use to monitor emerging risks? What early warning mechanisms exist, and how effective are they? How, and how often, are they calibrated?
- What is the role of technology in the risk management program? How was it chosen, and when was it last evaluated?
- What is the role of the tax function in the risk management program? Are we taking steps to demystify tax by gaining a high-level understanding of not only the downside consequences of tax risks, but also the upside potential that a robust tax risk management program can offer?

Area of focus 2: Foster a Risk Intelligent culture

In a Risk Intelligent culture, people at every level manage risk as an intrinsic part of their jobs. Rather than being risk averse, they understand the risks of any activity they undertake and manage them accordingly. Such a culture supports open discussion about uncertainties, encourages employees to express concerns, and maintains processes to elevate concerns to appropriate levels.

Actions to consider in fostering a Risk Intelligent culture:

- *Lead by example in communicating about risk.* The risk committee should ask management about the risks of specific decisions, activities, and initiatives. It should set expectations with senior executives and business unit leaders about what information the committee expects and how it will be conveyed. The committee should set the tone for an open and candid dialogue. Also, the risk committee has to work with management to develop appropriate messaging about the risk environment for the rest of the organisation.
- *Build cohesive teams with management.* Culture change occurs not by decree but through interactions with management. The committee should create opportunities to engage with management and to learn more about their risk management practices. These interactions can form the basis of a continual, interactive process of alignment that both allows the committee to refine its views and priorities, and enables management to adjust its practices to reflect your guidance.
- *Reward Risk Intelligent behaviour.* The risk committee should consider incorporating risk-related objectives into the company's executive remuneration structures. It may also wish to urge management to weave risk management practices into job descriptions, training, work processes, supervisory procedures, and performance appraisals.
- *Consider a third-party assessment.* In addition to self-assessment, commissioning an independent external review of the risk governance policies, procedures, and performance can yield useful benchmarking information and shed light on leading risk governance practices.

Questions to ask about the organisational culture:

- How are we communicating our Risk Intelligence messages and assessing the extent to which Risk Intelligence is understood throughout the enterprise?
- Are people comfortable in discussing risk, or are they afraid to raise difficult issues? How quickly do they raise issues?
- How might our remuneration programs encourage inappropriate short-term risk taking? How can we change these programs to encourage Risk Intelligent risk-taking instead? What mechanisms exist to recover remuneration when excessive risk-taking occurs?
- Has the organisation developed a common language around risk that defines risk-related terms and measures and that promotes risk awareness in all activities and at all levels?
- How have we demonstrated the significance of risk governance in our documentation and communications?
- What tools are we using to gauge our risk governance effectiveness, and with what results? What benefit might we derive from an independent evaluation?

Area of focus 3: Help management incorporate Risk Intelligence into strategy

Since one of a board's main responsibilities is to oversee the strategy-setting process, helping management incorporate Risk Intelligence into strategy is an inherent part of the risk committee's overall role. Drawing on a solid practical understanding of the enterprise's efforts around value creation and preservation, the committee can work with management to collaboratively move from a negative "incident" view of risk to a more positive "portfolio" view that considers risks and rewards in a broader strategic context.

Actions to consider in helping management incorporate Risk Intelligence into strategy:

- *Design processes for integrating risk management into strategic planning.* The committee may consider augmenting the overall strategic planning process with processes for considering risks across the organisation, prioritising the risks, and appropriately allocating risk management resources. It should consider the scenario-planning process and whether it incorporates both upside and downside risks, as well as a view into the overall risk exposures and opportunities. The committee may wish to develop processes that help verify that risk management incorporates value creation as well as preservation, that the risk appetite is defined and risk tolerances are identified, and that risk is handled accordingly. Also, the risk committee can include discussions about risk at retreats devoted to strategy.
- *Monitor strategic alignment.* Monitoring strategic alignment involves analysing the risk-return trade-off in setting the company's financial goals, the proposed means of reaching those goals, and likely constraints. To execute this monitoring, the risk committee will need to maintain visibility in strategic planning and risk-reward decisions. The committee must make it clear that any changes or events with potentially significant consequences for the organisation's reputation, as well as its financial position, are to be brought to its attention for consideration.

- *Establish accountability.* The risk committee should establish and reinforce executive accountability for risk management. One way to do this is to expect full disclosure by management of the risks associated with each aspect of the strategy. Give management on-going feedback about your satisfaction with their level of disclosure and the quality of risk-reward analyses. A formal evaluation process for specific executives, led by the chair of the risk committee may be considered.

Questions to ask when helping management incorporate Risk Intelligence into strategy:

- How can we build Risk Intelligence into decisions about capital allocation, acquisition, succession planning, and other strategic initiatives?
- How should risk-return trade-offs be weighed in strategic planning and review sessions? How can we generate more meaningful discussion of these trade-offs?
- What is the process for identifying and evaluating changes in the external environment? How are these findings considered in strategic planning?
- How realistic is the strategy? Under what scenarios would the strategy be achieved - or fail to be achieved – and what are the intended results or plans if it fails?
- What would it take - in resources, knowledge, alliances, or conditions - to increase the likelihood of achieving the desired results and to reduce the chances of failure?

Area of focus 4: Help define the risk appetite

Risk appetite defines the level of enterprise-wide risk that leaders are willing to take (or not take) with respect to specific actions, such as acquisitions, new product development, or market expansion. Where quantification is practical, risk appetite is usually expressed as a monetary figure or as a percentage of revenue, capital, or other financial measure (such as loan losses); however, we recommend that less quantifiable risk areas, such as reputational risk, also be considered when setting risk appetite levels. While the CEO proposes risk appetite levels, the risk committee on behalf of the board ought to approve them - or challenge them and send them back to the CEO for adjustments - based on an evaluation of their alignment with business strategy and stakeholders' expectations.

Risk appetites may vary according to the type of risk under consideration. Using a Risk Intelligent approach, companies ought to have an appetite for rewarded risks such as those associated with new product development or new market entry, and a much lower appetite for unrewarded risks such as non-compliance or operational failures. Some risks just come with the territory. If you are in the chemical business, there will inevitably be environmental spills and health and safety incidents. If you don't have the appetite for those types of risks, then you probably shouldn't be in that business. Once you have accepted this reality, you should do everything to prevent, rapidly detect, correct, respond to, and recover from any such incident.

Once the risk appetite is defined, management then should define specific risk tolerances, also known as risk targets or limits, that express the specific threshold level of risk by incident in terms that decision-makers can use (for instance, in completing an acquisition, the risk tolerance may be defined as a stop-loss threshold of a specified value). Management may have no tolerance for unethical business conduct or for environmental, health and safety incidents by adopting a zero incidents policy.

One important management responsibility is to continually monitor the company's risk exposures, evaluate actual risk exposure levels against the stated risk appetite, and adjust risk tolerances and policies as necessary to align actual risk exposure with the desired risk exposure as defined by the risk appetite. By having management report on this process to the risk committee, members can gain insight into whether there may be opportunities for further risk-for-reward strategies or, conversely, if the organisation is overly "stretched" in its risk levels.

Actions to consider in helping to define the risk appetite:

- *Distinguish between risk appetite and risk tolerance.* Many business unit leaders and some senior executives fail to distinguish between risk appetite and risk tolerance. As a result, many organisations either set arbitrary risk tolerances that do not track back to an overall risk appetite, or wrongly assume that a general statement of risk appetite gives decision-makers enough operational guidance to stay within its parameters. The risk committee can help the organisation steer clear of these traps by assisting management in developing a cogent approach to defining the risk appetite, specifying risk tolerances, and communicating them across the enterprise.
- *Serve as a sounding board.* The committee should be available as a resource for helping senior executives understand and reconcile various views of risk within the organisation. One way to do this is to ascertain how management balances and aggregates the business units' risks as well as how management sets various risk tolerances, particularly in relatively risky businesses or markets.

Questions to ask regarding risk appetite:

- What size risks or opportunities do we expect management to bring to our attention?
- How does management determine the organisation's risk appetite? Which risk categories are considered, and how do they relate to management's performance goals and compensation metrics?
- In developing the risk appetite, how did management incorporate the perspectives of shareholders, regulators, and analysts — and experiences of peer companies?
- How are risk tolerances set? How does that process account for risk appetite? How do risk tolerances relate to the risk appetite and to risk categories?
- What scenario-planning or other models are used in setting the risk appetite and tolerances? How do these tools account for changing circumstances and for the human factor?

Companies ought to have an appetite for rewarded risks... and a much lower appetite for unrewarded risks.

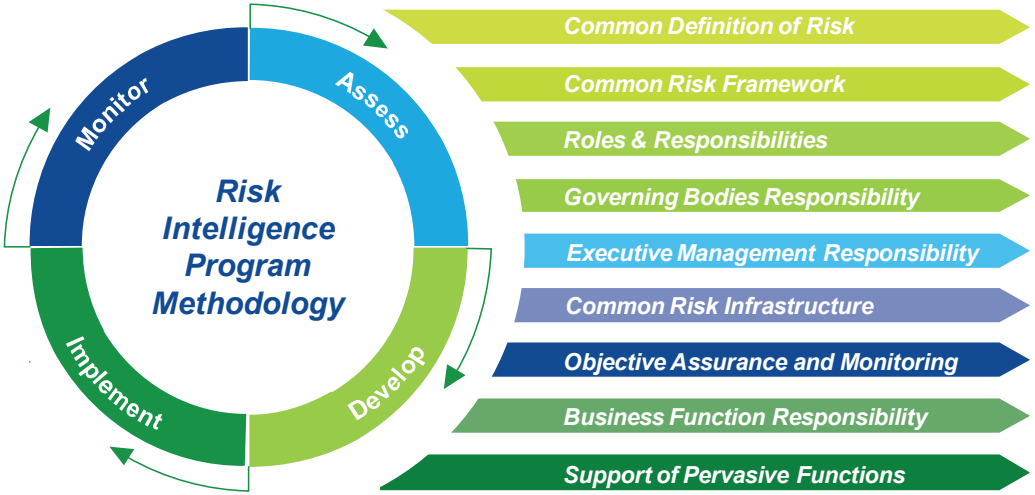
Area of focus 5: Execute the Risk Intelligent governance process

A Risk Intelligent governance process should be strategic in design, promote awareness of the relationship between value and risk, and efficiently and effectively allocate the company's risk management resources. Effective execution of the process depends on maintaining a disciplined, collaborative approach focused on process design, process monitoring, and accountability.

Actions to consider in executing the Risk Intelligent governance process:

- *Work with management on process design*. A joint approach to process design can help establish processes that both the risk committee and management feel are effective, yet not overly burdensome. The committee can collaborate with executives to develop value creation and risk management objectives, board responsibilities, and mechanisms for elevating key risk issues. It's often useful to establish policies that detail the circumstances under which management must obtain board or committee approval for decisions, while noting that the board's role is risk governance rather than risk management.
- *Monitor the overall risk management process.* The risk committee should set up procedures for evaluating and overseeing the processes by which risks are systematically identified, reported, and managed. To execute effective monitoring, it's important that committee members keep abreast of the company's vulnerabilities, risk appetite, and risk tolerances; understand the risk management system; and bring an integrated view of the organisation's risk management methods to discussions with the executive team.
- *Conduct formal risk management program assessments*. A risk management program assessment can include questions about risk governance, risk infrastructure and management, and risk ownership. This provides a comprehensive view of the process and enables all stakeholders to see how they fit into both the basic process and any improvement efforts.

- *Clarify accountability at the board and management levels.* Complete, on-going disclosure of major risk exposures by the CEO to the committee and the board is fundamental to a Risk Intelligent governance process. We suggest that that committee works with the CEO to verify that responsibility for specific risks and related activities has been assigned to specific members of the management team. In doing this, it's important for the committee and the CEO to maintain a constructive, collaborative relationship — but that need not stop the risk committee from discussing difficult issues with management and questioning practices when doubts arise.



It's important for the risk committee and the CEO to maintain a constructive, collaborative relationship.

Questions to ask when executing the governance process:

- Are people at all levels — across silos — actively engaged in risk management? If so, how? If not, why not?
- What criteria does management use to prioritise enterprise risks? How well does the company's allocation of risk management resources align with those priorities?
- How is management addressing the major opportunities and risks facing the company? How do we know that these are, in fact, the major opportunities and risks, and that the steps management is taking to address them are appropriate?
- How do we know when risks are increasing, holding steady, or decreasing? What processes does management use to identify and monitor these trends over time?
- How often do we discuss risk with management? What issues have been brought to our attention in the past six to twelve months?

Notes:

Area of focus 6: Benchmark and evaluate the governance process

Risk governance is a continual process, and systematic mechanisms for evaluating and improving risk governance proficiency can greatly benefit efforts to identify, prioritise, and implement improvements as well as give the risk committee visibility into the organisation's progress toward a Risk Intelligent governance approach. Such mechanisms allow the committee to gauge the institution's current stage of development relative to peers; they can also help track the progress of the governance program along a Risk Intelligence "maturity model." As it is good practice to obtain periodic independent assessment of the risk management process, King III requires that Internal Audit provide a written assessment of the risk management function to the Board.

Actions to consider in benchmarking and evaluating the governance process:

- *Use internal monitoring and feedback.* The risk committee should periodically ask for feedback from senior executives on how well the committee and other board members have played their risk oversight role. As part of this effort, the committee may consider the report from Internal Audit on the effectiveness of the risk management process. The committee may also wish to request relevant reports from the risk management team. The committee may also review the methods by which management assesses the risk management program.
- *Participate in continuing education and updates.* To keep individual committee members' knowledge up to date, it's helpful to receive on-going updates on approaches to risk management and on risks developing in the internal and external environment.
- *Solicit independent viewpoints*. An independent review of the risk governance program can help to identify what is working, locate any gaps, and prioritise areas for improvement. The committee should consider having management present the summary results along with a plan for any corrective actions.

- *Include risk as a topic in the annual board self-assessment.* The board's annual self-assessment process provides a broad view into how the full board feels that it is performing in its overall governing body role. Including questions in the assessment form focused specifically on risk governance effectiveness can be a valuable guide to measuring the committee and the individual members' effectiveness in providing Risk Intelligent governance. The nominations committee may wish to consider reviewing the assessment form to verify that it includes such language.

Questions to ask when benchmarking and evaluating the governance process:

- How have we gone about assessing our risk governance and management programs? What other tools might we use in this assessment?
- To what extent are our compliance, internal audit, and risk management teams employing Risk Intelligent approaches? How are risks aggregated across our businesses?
- What value might we derive by engaging a third party to assess our organisation against leading practices, industry peers, and other benchmarks?
- How can we improve our risk governance proficiency, stay current, and share knowledge about risk governance - both individually and collectively?
- What steps can we take to improve the quality of our risk governance and management processes?

Ask for feedback from senior executives on how well you and your fellow board members have played your risk oversight role.

Section 5

On-going education and periodic evaluation

As with other board responsibilities, it is important that risk oversight does not become a set-it-and-forget-it proposition. Risks in the economic, competitive, regulatory, legal, and technological environments are dynamic, and risk governance must evolve in response.

Education never ends

In terms of King III, companies should ensure the continued education of all board members with the intention of keeping them up to date with applicable prescripts and best practice. As a committee dealing with an area in constant flux, the risk committee should consider how it plans to stay informed about developments in risk management practices and emerging risk areas.

The following guidelines can assist risk committees in developing education and training initiatives to:

- Stay abreast of leading practices as risks evolve and as management updates its risk management methods.
- Understand new risks associated with new businesses and locations and how changes in regulations in foreign jurisdictions can increase or decrease risk.
- Periodically benchmark risk governance practices of peers (including peer companies within the company's industry), competitors, customers, and suppliers in order to understand evolving practices and evolving expectations of business partners and investors.
- Keep up to date on risk disclosure requirements in external/public communications.
- Offer orientation programs for new risk committee members and a module in board members' orientations to inform them about the risk committee.

Education could include sources ranging from conferences and continued readings to courses designed for senior executives to customised briefings from external specialists. Deloitte suggests a mix of general updates and company-specific information on risk, risk governance, and risk management.

Evaluations are a must

King III stresses that the evaluation of the board, its committees and the individual directors should be performed every year. Effective and meaningful evaluation is only possible once the board has determined its own role, functions, duties and performance criteria as well as those for the board committees.

The performance of the risk committee as a whole and, possibly, that of individual members should be evaluated periodically.

- Areas of risk committee performance to consider evaluating may include:
  - Breadth and depth of the committee's knowledge of risk and risk governance and management (including on-going education)
  - Independence of the risk committee members from management
  - Performance of the chair of the committee and his or her relations with management, the CEO, the CRO and with the committee
  - Clarity of communications with management about risk and the degree to which these communications have been understood and acted upon
  - Quality of board, risk committee, and management responses to potential or actual financial, operational, regulatory, or other risk events
  - Effectiveness of the information received and reporting about risk by management
- There are several methods for board committee evaluations, each with its advantages and disadvantages:
  - Self-evaluation
  - Peer evaluation
  - External evaluation
- In the absence of regulations to the contrary, an annual self-evaluation of the risk committee as a whole, as well as an evaluation conducted with external specialists every two or three years may be beneficial and appropriate.

Tools and resource. To assist risk committees in their evaluation efforts, we have included a sample risk committee performance evaluation questionnaire in Appendix C.

Ever vigilant, continually improving

Much of the value of the risk committee will likely come from the questions it poses, such as the following two, which are central to risk oversight:

- What are all the risks of a decision or initiative — for instance, of a new product, market, acquisition, or financial structure — that management may be considering?
- What steps has management taken to mitigate, manage, and monitor those risks?

Developments in the business, financial, economic, and regulatory environment can be expected to subject risk committees to an expanding range of responsibilities, up to and including weighing in on strategic issues from a risk-oversight perspective. While the full board takes the lead in strategy discussions with the executive team, the risk committee often will have a valuable wide – angle perspective to offer to the board.

Regardless of how the committee's responsibilities evolve, a key skill of its members will be to understand and prioritise the risk governance and oversight needs of the enterprise. This can require at least as much wisdom as skill. By that we mean committee members must understand the risks posed by the business itself and by external forces and how they might affect the enterprise.

Then, as appropriate, they should question management about the risks and about how the organisation is addressing them. Then they must listen carefully to the answers and, as appropriate, probe for more information.

Further information may come from internal, financial, audit, or assurance reports and from informal conversations with the CRO and members of the management risk committee. In fact, when failures in risk management occur, in Deloitte's experience, post-incident reviews of "What happened?" often reveal that information which could have helped the enterprise recognise the risk sooner and address it more effectively already existed within the organisation.

This knowledge presents risk committees with a real opportunity. They can shoulder the responsibility of helping management to identify not only risks (and opportunities) and ways of addressing them, but also ways of improving the risk management infrastructure so that information about risks and how to manage them surfaces before, rather than after, risk events.

Questions to ask to encourage continual improvement in risk oversight:

- How do we evaluate the CEO, CFO, chief audit executive, and other senior positions in terms of their risk awareness and approach to risk management?
- How are we working with management and stakeholders (especially shareholders) to help the enterprise balance demands for short-term performance and long-term prosperity?
- What are our ethical and legal responsibilities for risk oversight in energy efficiency, water usage, labour practices, and other areas of sustainability, and how are we meeting them?
- Where is the line between risk oversight and risk management? How do we practice the right balance that characterises sound risk governance?
- What assurance is the risk committee obtaining on the effectiveness of the risk management function?
- How embedded is the risk culture within the organisation?
- How do we keep the risk committee from becoming stale, set in its ways, or merely pro forma in its approach to oversight? How do we stay open to opportunities to improve when we believe our methods are working?

Appendix A

This sample risk committee charter is based on leading practices observed by Deloitte in the analysis of a variety of materials.

It is important to note that the Risk Committee Resource Guide practices are drawn from Deloitte experiences and our understanding of practices currently being used.

Deloitte does not accept any responsibility for any errors this publication may contain, whether caused by negligence or otherwise, or for any losses, however caused, sustained by any person that relies on it. The information presented can and will change; we are under no obligation to update such information. Deloitte makes no representations as to the sufficiency of these tools for your purposes, and, by providing them, we are not rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. These tools should not be viewed as a substitute for such professional advice or services, nor should they be used as a basis for any decision that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional adviser.

Deloitte does not assume any obligations as a result of your access to or use of these tools.
This template is designed for South African public companies; exceptions to the requirements noted below may apply for certain issuers, including investment companies, small-business issuers, and foreign private issuers. All companies should consult with legal counsel regarding the applicability and implementation of the various requirements identified. Further, this template should be tailored on a company-by-company basis to meet the needs and specific situations for each company utilising the tool.

Sample risk committee charter

I. Purpose and authority

The risk committee is established by and among the board to properly align with management as it embarks a risk management program. The primary responsibility of the risk committee is to oversee and approve the company-wide risk management practices to assist the board in:

- Overseeing that the executive team has identified and assessed all the risks that the organisation faces and has established a risk management infrastructure capable of addressing those risks
- Overseeing, in conjunction with other board-level committees or the full board, if applicable, risks, such as strategic, financial, credit, market, liquidity, security, property, IT, legal, regulatory, reputational, and other risks
- Overseeing the division of risk-related responsibilities to each board committee as clearly as possible and performing a gap analysis to determine that the oversight of any risks is not missed
- In conjunction with the full board, approving the company's enterprise wide risk management framework

The risk committee may have the authority to conduct investigations into any matters within its scope of responsibility and obtain advice and assistance from outside legal, accounting, or other advisors, as necessary, to perform its duties and responsibilities.

In carrying out its duties and responsibilities, the risk committee shall also have the authority to meet with and seek any information it requires from employees, officers, directors, or external parties. In addition, the risk committee could make sure to meet with other board committees to avoid overlap as well as potential gaps in overseeing the companies' risks.

The risk committee will primarily fulfil its responsibilities by carrying out the activities enumerated in Section III of this charter.

II. Composition and meetings

The risk committee will comprise three or more directors as determined by the board. The membership will include a combination of executive and non-executive directors. The committee may include non-directors as members. Each member will have an understanding of risk management expertise commensurate with the company's size, complexity and capital structure.

The risk committee will provide its members with annual continuing education opportunities and customised training focusing on topics such as leading practices with regard to risk governance and oversight and risk management.

Committee members will be appointed by the board. Unless a chairperson is elected by the full board, the members of the committee may designate a chairperson by majority vote. Additionally, the risk committee, in conjunction with the full board and with the nominations committee, may do well to consider and plan for succession of risk committee members.

The risk committee will report to the full board. The risk committee will consider the appropriate reporting lines for the CEO, the company's chief risk officer (CRO) and the company's management-level risk committee - whether indirectly or directly - to the risk committee.

The committee will meet at least quarterly, or more frequently as circumstances dictate. The committee chairperson will approve the agenda for the committee's meetings, and any member may suggest items for consideration. Briefing materials will be provided to the committee as far in advance of meetings as practicable.

Each regularly scheduled meeting will begin or conclude with an executive session of the committee, absent members of management. As part of its responsibility to foster open communication, the committee will meet periodically with management, heads of business units, the CRO (if applicable), the chief audit executive (director of the internal audit function), and the independent auditor in separate executive sessions.

III. Responsibilities and duties

To fulfil its responsibilities and duties, the risk committee will:

Enterprise responsibilities

- Help to set the tone and develop a culture of the enterprise vis-à-vis risk, promote open discussion regarding risk, integrate risk management into the organisation's goals and compensation structure, and create a corporate culture such that people at all levels manage risks rather than reflexively avoid or heedlessly take them
- Provide input to management regarding the enterprise's risk appetite and tolerance and, ultimately, approve risk appetite and the statement of risk appetite and tolerance messaged throughout the company and by line of business
- Monitor the organisation's risk profile - its on-going and potential exposure to risks of various types
- Approve the risk management policy and plan. Management should develop both the risk management policy and the plan for approval by the committee. The risk management plan should consider the maturity of the risk management of the company and should be tailored to the specific circumstances of the company. The risk management plan should include:
  - the company's risk management structure
  - the risk management framework i.e. the approach followed, for instance, COSO, ISO, IRMSA ERM Code of Practice, etc.
  - the standards and methodology adopted – this refers to the measureable milestones such as tolerances, intervals, frequencies, frequency rates, etc.
  - risk management guidelines
  - reference to integration through, for instance, training and awareness programmes, and
  - details of the assurance and review of the risk management process.

The risk management policy should set the tone for risk management in the company and should indicate how risk management will support the company's strategy. The risk management policy should include the compa¬ny's definitions of risk and risk management, the risk management objectives, the risk approach and philosophy, as well as the various responsibilities and ownership for risk management within the company.

- The committee should review the risk management plan at least once a year.
- Define risk review activities regarding the decisions (e.g. acquisitions), initiatives (e.g. new products), and transactions and exposures (e.g. by amount) and prioritise them prior to being sent to the board's attention
- Review and confirm that all responsibilities outlined in the charter have been carried out
- Monitor all enterprise risks; in doing so, the committee recognises the responsibilities delegated to other committees by the board and understands that the other committees may emphasise specific risk monitoring through their respective activities
- Conduct an annual performance assessment relative to the risk committee's purpose, duties, and responsibilities; consider a mix of self- and peer- evaluation, supplemented by evaluations facilitated by external experts
- Oversee the risk program/interactions with management
- Review and approve the risk management infrastructure and the critical risk management policies adopted by the organisation
- Periodically review and evaluate the company's policies and practices with respect to risk assessment and risk management and annually present to the full board a report summarising the committee's review of the company's methods for identifying, managing, and reporting risks and risk management deficiencies
- Continually, as well as at specific intervals, monitor risks and risk management capabilities within the organisation, including communication about escalating risk and crisis preparedness and recovery plans
- Continually obtain reasonable assurance from management that all known and emerging risks have been identified and mitigated or managed
- Communicate formally and informally with the executive team and risk management regarding risk governance and oversight

- Discuss with the CEO and management the company's major risk exposures and review the steps management has taken to monitor and control such exposures, including the company's risk assessment and risk management policies
- Review and assess the effectiveness of the company's enterprise-wide risk assessment processes and recommend improvements, where appropriate; review and address, as appropriate, management's corrective actions for deficiencies that arise with respect to the effectiveness of such programs
- Monitor governance rating agencies and their assessments of the company's risk and proxy advisory services policies, and make recommendations as appropriate to the board
- In coordination with the audit committee, understand how the company's internal audit work plan is aligned with the risks that have been identified and with risk governance (and risk management) information needs

Reporting

- Understand and approve management's definition of the risk-related reports that the committee could receive regarding the full range of risks the organisation faces, as well as their form and frequency
- Respond to reports from management so that management understands the importance placed on such reports by the committee and how the committee views their content
- Read and provide input to the board and audit committee regarding risk disclosures in financial statements and other public statements regarding risk
- Keep risk on both the full board's and management's agenda on a regular basis
- Coordinate (via meetings or overlap of membership), along with the full board, relations and communications with regard to risk among the various committees, particularly between the audit and risk committees
- Disclose in the company's Integrated Report how it has satisfied itself that risk assessments, responses and interven¬tions are effective

Charter review

- Review the charter at least annually and update it as needed to respond to new risk-oversight needs and any changes in regulatory or other requirements
- Review and approve the management-level risk committee charter, if applicable
- Perform any other activities consistent with this charter, the company's bylaws, and governing laws that the board or risk committee determines are necessary or appropriate
- Submit the charter to the full board for approval

Notes:

Appendix

B

Illustrative planning tool: Risk committee calendar of activities

Risk committees can use this tool to help plan their annual activities and meeting agendas. This tool is current, based on our understanding of the common practices in the marketplace. The action or responsibility, as described, may not be an explicit legislative or regulatory requirement or proposal, but may be an action that may result from legislative or regulatory requirements or proposals.

The "Suggested Frequency" section offers a suggestion for how often the activity could be performed, while the "Meeting Month" section provides an area where the risk committee can mark the months in which an activity could be performed. The risk committee might use this tool in conjunction with the "sample risk committee charter," and it should be tailored to reflect the responsibilities in the company's risk committee charter.

This document is not an all-inclusive list of activities that a risk committee should or must execute. The planning tool contains general information only and does not constitute, and should not be regarded as, legal or similar professional advice or service. Deloitte does not accept any responsibility for any errors this publication may contain, whether caused by negligence or otherwise, or for any losses, however caused, sustained by any person that relies on it. The information presented can and will change; we are under no obligation to update such information. Deloitte makes no representations as to the sufficiency of these tools for your purposes, and, by providing them, we are not rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. These tools should not be viewed as a substitute for such professional advice or services, nor should they be used as a basis for any decision that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional adviser. Deloitte does not assume any obligations as a result of your access to or use of these tools.

This planning tool is designed for use by SA public companies. All companies should consult with legal counsel regarding the applicability and implementation of the various activities identified.

Action/Responsibility	Suggested frequency	Meeting month												Comments
		January	February	March	April	May	June	July	August	September	October	November	December	
Enterprise Responsibility														
Help to set the tone and develop a culture of the enterprise vis-à-vis risk, and promote open discussion regarding risk, integrate risk management into the organisation's goals and compensation structure, and create a corporate culture such that people at all levels manage risks rather than reflexively avoid or heedlessly take them.	Continuously													
Provide input to management regarding the enterprise's risk appetite and tolerance and, ultimately, approve risk appetite and the statement of risk appetite and tolerance messaged throughout the company and by line of business	Annually													
Monitor the organisation's risk profile — its on-going and potential exposure to risks of various types	Continuously													
Define risk review activities regarding the decisions (e.g., acquisitions), initiatives (e.g., new products), and transactions and exposures (e.g., by amount) and prioritise them prior to being sent to the board's attention	Annually and as needed													
Oversee the risk programme/interactions with management														
Review and confirm that all the responsibilities outlined in the charter have been carried out.	Continuously													
Monitor all enterprise risks; in doing so, the committee recognises the responsibilities delegated to other committees by the board and understands that the other committees may emphasis specific risk monitoring through their respective activities.	Annually and as needed													
Conduct an annual performance assessment relative to the risk committee's purpose, duties, and responsibilities; consider a mix of self- and peer evaluation, supplemented by evaluations facilitated by external experts	Annually													
Review and approve the risk management infrastructure and the critical risk management policies adopted by the organisation	Annually													

Periodically review and evaluate the company's policies and practices with respect to risk assessment and risk management and annually present to the full board a report summarising the committee's review of the company's methods for identifying and managing risks and reporting risks and risk management deficiencies	Annually and as needed													
Continually, as well as at specific intervals, monitor risks and risk management capabilities within the organisation, including communications about escalating risk and crisis preparedness and recovery plans	Continuously													
Continually obtain reasonable assurance from management that all known and emerging risks have been identified and mitigated or managed	Continuously													
Communicate formally and informally with the executive team and risk management regarding risk governance and oversight	Continuously													
Discuss with management and the CRO the company's major risk exposures and review the steps management has taken to monitor and control such exposures, including the company's risk assessment and risk management policies	Continuously													
Review and assess the effectiveness of the company's enterprise-wide risk assessment processes and recommend improvements, where appropriate; review and address as appropriate management's corrective actions for deficiencies that arise with respect to the effectiveness of such programs	Annually and as needed													
Monitor governance rating agencies and their assessments of the company's risk and proxy advisory services policies, and make recommendations as appropriate to the board	Annually and as needed													
In coordination with the audit committee, understand how the internal audit work plan is aligned with the risks that have been identified and with risk governance (and risk management) information needs	Annually													

Chief risk officer														
Ensure that the company's CRO (if applicable) has sufficient stature, authority, and seniority within the organisation and is independent from individual business units within the organisation	Annually and as needed													
If the CRO reports to the risk committee, review the appointment, performance, and replacement of the CRO of the company in consultation of the nomination and governance committee and the full board	Each board meeting													
Reporting														
Understand and approve management's definition of the risk-related reports that the committee should receive regarding the full range of risks the organisation faces, as well as their form and frequency of such reports	Annually and as needed													
Respond to reports from management so that management understands the importance placed on such reports by the committee and how the committee views their content	Annually and as needed													
Read and provide input to the board and audit committee regarding risk disclosures in financial statements, proxy statements, and other public statements regarding risk	Annually													
Keep risk on both the full board's and management's agenda on a regular basis	Continuously													
Coordinate (via meetings or overlap of membership), along with the full board, relations and communications with regard to risk among the various committees, particularly between the audit and risk committees	Continuously													

Charter review														
Review the charter at least annually and update it as needed to respond to new risk-oversight needs and any changes in regulatory or other requirements	Annually and as needed													
Review and approve the management-level risks committee charter, if applicable	Annually													
Perform any other activities consistent with the charter, the company's bylaws, and governing laws that the board or risk committee determines are necessary or appropriate	Continuously													
Submit the charter to the full board for approval	Annually													

Notes:

Appendix

C

Risk committee performance evaluation

While there is currently not a legal or regulatory requirement for board risk committees to complete a performance evaluation, King III recommends regular performance evaluations for all board committees. Based on our knowledge, assessing committee performance on a regular basis is a leading governance practice.

Areas of risk committee performance to be evaluated may include:

- Breadth and depth of the committee's knowledge of risk and risk governance and management (including on-going education)
- Independence of the risk committee members from management
- Performance of the chair of the committee and his or her relations with management and the chief risk officer (CRO), and with the committee
- Clarity of communications with management about risk and the degree to which these communications have been understood and acted upon
- Quality of board, risk committee, and management responses to potential or actual financial, operational, regulatory, or other risk events
- Effectiveness of the information received by the risk committee and reporting about risk by management
- Engagement with regulators and others on risk management-related matters

There are several methods for board committee evaluations, each with its advantages and disadvantages:

- Self-evaluation
- Peer evaluation
- External evaluation

In the absence of regulations to the contrary, an annual self-evaluation of the risk committee as a whole, as well as an evaluation conducted with external specialists every two or three years may be beneficial and appropriate.

The following questionnaire is based on our knowledge and understanding of emerging and leading practices and is designed to assist in the self-assessment of a risk committee's performance. It is not intended to be all inclusive and, if used, should be modified to accommodate a company's specific circumstances.

When completing the performance evaluation, consider the following process:

- Select a coordinator and establish a timeline for the process
- In addition to risk committee members completing the form as a self-evaluation, ask individuals who interact with the risk committee members to provide feedback
- Ask each risk committee member to complete an evaluation by selecting the appropriate rating that most closely reflects the risk committee's performance related to each practice
- Consolidate the results of such inquiry and evaluation into a summarised document for discussion and review by the committee

Sample evaluation questionnaire

For each of the following statements, select a number between 1 and 5, with 1 indicating that you strongly disagree and 5 indicating that you strongly agree with the statement. Select 0 if the statement is not applicable or you do not have enough knowledge or information to rank the organisation's risk committee on a particular statement.

Circle one number for each statement	Insufficient knowledge	Strongly disagree	Neither agree nor disagree			Strongly agree
Composition and quality						
1. The designated risk expert meets the definition of "expert" as agreed to by the committee and the board.	0	1	2	3	4	5
2. Risk committee members have the appropriate qualifications to meet the objectives of the risk committee's charter, including appropriate risk background/qualifications.	0	1	2	3	4	5
3. The risk committee demonstrates integrity, credibility, trustworthiness, active participation, an ability to handle conflict constructively, strong interpersonal skills, and the willingness to address issues proactively.	0	1	2	3	4	5
4. The risk committee demonstrates appropriate industry knowledge and includes a diversity of experiences and backgrounds.	0	1	2	3	4	5
5. The risk committee participates in a continuing education program to enhance its members' understanding of relevant risk management and industry-specific issues.	0	1	2	3	4	5
6. The risk committee reviews its charter annually to determine whether its responsibilities are described adequately and recommends changes to the board for approval.	0	1	2	3	4	5
7. New risk committee members participate in an orientation program to educate them on the company, their responsibilities, and the company's risk management and oversight policies and practices.	0	1	2	3	4	5
8. The risk committee chairman is an effective leader.	0	1	2	3	4	5
9. The risk committee, in conjunction with the nominations, creates a succession and rotation plan for risk committee members, including the risk committee chairman.	0	1	2	3	4	5

Circle one number for each statement	Insufficient knowledge	Strongly disagree	Neither agree nor disagree			Strongly agree
Understanding the business and associated risks						
1. The risk committee oversees or knows that the full board or other committees are overseeing significant risks that may directly or indirectly affect the company. Examples include: • Regulatory and legal requirements • Concentrations (e.g., suppliers and customers) • Market and competitive trends • Financing and liquidity needs • Financial exposures • Business continuity • Company reputation • Financial strategy execution • Financial management's capabilities • Management override • Fraud control • Company pressures, including "tone at the top"	0	1	2	3	4	5

Circle one number for each statement	Insufficient knowledge	Strongly disagree	Neither agree nor disagree			Strongly agree
Understanding the business and associated risks						
2. The risk committee discusses the company's risk appetite and specific risk tolerance levels in conjunction with strategic objectives, as presented by management, at least annually.	0	1	2	3	4	5
3. The risk committee considers, understands, and approves the process implemented by management to effectively identify, assess, monitor, and respond to the organisation's key risks.	0	1	2	3	4	5
4. The risk committee understands and approves management's fraud risk assessment and has an understanding of identified fraud risks.	0	1	2	3	4	5
5. The risk committee considers the company's performance versus that of its peers in a manner that enhances comprehensive risk oversight by using reports provided directly by management to the risk committee or at the full board meeting.	0	1	2	3	4	5
Process and procedures						
6. The risk committee reports its proceedings and recommendations to the board after each committee meeting.	0	1	2	3	4	5
7. The risk committee develops a calendar that dedicates the appropriate time and resources needed to execute its responsibilities.	0	1	2	3	4	5
8. Risk committee meetings are conducted effectively, with sufficient time spent on significant or emerging issues.	0	1	2	3	4	5
9. The level of communication between the risk committee and relevant parties is appropriate; the risk committee chairman encourages input on meeting agendas from committee and board members and senior management, including CEO, CFO, CRO, CIA, CCO, and business-unit leaders.	0	1	2	3	4	5
10. The risk committee sets clear expectations and provides feedback to the full board concerning the competency of the organisation's CRO and the risk management team.	0	1	2	3	4	5
11. The risk committee has input into the succession planning process for the CRO.	0	1	2	3	4	5
12. The agenda and related information (e.g., prior meeting minutes, reports) are circulated in advance of meetings to allow risk committee members sufficient time to study and understand the information.	0	1	2	3	4	5

Circle one number for each statement	Insufficient knowledge	Strongly disagree	Neither agree nor disagree			Strongly agree
13. Written materials provided to risk committee members are relevant and at the right level to provide the information the committee needs to make decisions.	0	1	2	3	4	5
14. Meetings are held with enough frequency to fulfil the risk committee's duties at least quarterly, which should include periodic visits to company locations with key members of management.	0	1	2	3	4	5
15. Regularly, risk committee meetings include separate private sessions with business-unit leaders, the CRO or equivalent, and the internal auditor.	0	1	2	3	4	5
16. The risk committee maintains adequate minutes of each meeting.	0	1	2	3	4	5
17. The risk committee meets periodically with the committee(s) responsible for reviewing the company's disclosure procedures (typically the audit committee) in order to discuss respective risk-related disclosures.	0	1	2	3	4	5
18. The risk committee coordinates with other board committees (e.g., audit committee) to avoid gaps or redundancy in overseeing individual risks.	0	1	2	3	4	5
19. The risk committee respects the line between oversight and management of risks within the organisation.	0	1	2	3	4	5
20. Risk committee members come to meetings well prepared.	0	1	2	3	4	5
Monitoring activities						
21. An annual performance evaluation of the risk committee is conducted, and any matters that require follow-up are resolved and presented to the full board.	0	1	2	3	4	5
22. The company provides the risk committee with sufficient funding to fulfil its objectives and engage external parties for matters requiring external expertise.	0	1	2	3	4	5
Communication activities						
23. The risk committee communicates regularly with regulators and others on risk management-related matters.	0	1	2	3	4	5

Appendix D

Board-level Risk Intelligence map

Critical areas and sample risks that the board should own and manage									
Board effectiveness/ knowledge management	**Board structure and leadership**	**Compensation/ performance incentives/ alignment**	**Corporate Responsibility & Sustainability (CR&S)**	**Reputation/ stakeholder relations**	**Risk-oversight**	**Transparency and financial integrity**	**Ethical culture/ tone at the top**	**Crisis management**	**CEO succession planning**
– Failure to understand and exercise fiduciary duties – Ineffective/ insufficient independent committees – Poor communication from management – Inadequate knowledge of board responsibilities – Inadequate understanding of the organisation's business – Limited exposure to management outside of the CEO and CFO – Lack of board cohesiveness	– Lack of appropriate tone at the top set by leadership – Weak structure/ composition of the board – Ineffective communication between and among the board and management – Board conflict of interest or lack of independence – Inappropriate decision-making and delegation of authorities – Poor cooperation and organisational alignment – Inadequate attention to strategy and execution	– Inadequate disclosure of compensation process and philosophies – Misalignment of performance metrics with long-term strategy – Executive compensation inconsistent with stakeholder expectations – Undue emphasis on the short-term results – Misalignment of incentives and rewards	– Failure to meet social responsibility obligations – Lack of involvement from appropriate levels of management – Inadequate oversight over CR&S activities – Lack of adequate disclosure of CR&S activities	– Inability to understand and meet shareholder expectations – Failure to understand trends related to the organisation's workforce, creditors, customers, and other stakeholders – Real or perceived influence of majority shareholders – Failure to adequately consider and/ or respond to shareholders proposals – Poor corporate brand perception	– Inadequate board oversight of risk management activities – Inadequate structure to allow for an enterprise risk management process – Inadequate or inappropriate risk appetite and tolerances – Lack of Risk Intelligent decision-making – Inadequate risk-related public disclosure – Inadequate utilisation of an appropriate risk framework – Lack of risk management expertise on the risk committee (or board)	– Cursory reviews of financial statements and related disclosures – Failure to challenge management assumptions – Inadequate oversight of internal and external auditors – Inadequate of unqualified finance organisation – Lack of financial expertise on the audit committee	– Failure to foster an ethical culture – Inappropriate performance incentives – Failure to monitor and control unauthorised activities – Failure to protect whistleblowers	– Lack of planning for management during crisis – No formal crisis management plan exists – Lack of definition of roles during crisis	– Lack of discussion or formal plan for CEO succession – Inadequate focus placed on recruitment, development and deployment of quality leadership

Representative questions that the board might ask in managing board-level risks			
Managing known risk areas		Identifying the unknown	
• Is there a common understanding of risk and opportunity? • Is there a common language to bridge risk and business silos? Is it ingrained into the risk framework? • How much can be gained by properly managing this risk? How much is it costing us (or will it cost us) to manage this risk? What is the cost of inaction? • What are the different ways in which value can be created or destroyed? • Does our risk management or mitigation strategy introduce any additional risks?	• What is the magnitude of the known risk exposures (inherent)? • Are any of these risk exposures life threatening to the enterprise? How fast can they occur? Are we prepared to respond/ recover? • How can we be confident of our risk management practices? What are the exposures (residual) despite them? • Are the residual exposures within the risk appetite of the firm? If not, what can we practicably do to reduce our exposure to these risks to an acceptable level? • Do we only conduct business within approved business areas, for approved product and transaction types, and with approved customers and counterparties?	• What are the risks arising out of the underlying assumptions in our strategy choices? What if the assumptions are wrong? • Do the underlying assumptions of our industry and enterprise pose some risks? • What are the assumptions underlying our value proposition and market segmentation? • Have the opposites of these assumptions been identified? What are the implications of these on our business?	• Can we detect significant changes in the environment (including regulatory changes) that affect our business model and its underlying assumptions? • What might be the unintended consequences of our decisions? Can we detect them? • Does the enterprise have common triggers to alert leadership to strategic changes? • Does bad news travel fast or have there been delays in escalating negative issues? • How do we monitor for potential new business activity, new transaction types, and new customers and counterparties?

Contacts

Dr Johan Erasmus

Tel: 082 573 2536
jerasmus@deloitte.co.za

Nina le Riche

Tel: 082 331 4840
nleriche@deloitte.co.za

Designed and produced by Creative Services at Deloitte, Johannesburg. (807472/ryd)