Deloitte.

Risk Committee Resource Guide for Boards

Contents

Foreword

In the past few years, Deloitte has seen board members in a wide range of industries stepping up their efforts to define and fulfill their risk governance responsibilities. In this process, a board may consider or establish a board-level risk committee. To assist in these efforts, Deloitte has prepared this guide, which fulfills a function similar to our Audit Committee Resource Guide, but for boards that are considering, establishing, or maintaining a board risk committee.

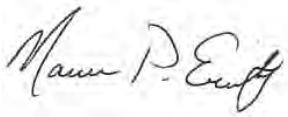
Given their industry and regulatory environment, a good number of major banks already have board risk committees. Risk committees will become more prevalent with the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank") which delegated the rule making to implement its broad policy goals to the Federal Reserve. Subsequently, the Federal Reserve issued its notice of proposed rule making (NPR) on enhanced prudential supervision which will require: 1) U.S. banks and bank holding companies (BHCs) with greater than $50 billion in assets; 2) those with greater than $10 billion in assets and that are publicly-traded; and 3) non-bank financial companies designated as systemically important to establish a board risk committee with a formal written charter approved by the company's board of directors. The NPR will further require for U.S. banks and bank holding companies with greater than $50 billion in assets and non-bank financial companies designated as systemically important that such board risk committees cannot be housed within another committee, must report directly to the board, and must receive and review regular reports from the Chief Risk Officer (CRO).

Boards of large non-bank financial companies as well as those of commercial enterprises recognize that their organizations are facing a broad range of risks, including, for example, strategic, security, property, information technology (IT), legal, regulatory, reputational, and other risks, as well as heightened financial risk. In any enterprise, risk governance means ascertaining, to a reasonable degree, that the executive team has identified and assessed critical risks and has appropriate risk mitigation and management in place that are designed to address the risks that the organization faces. This is a critical responsibility of many boards. To reinforce the importance of risk governance, the U.S. Securities and Exchange Commission (SEC) issued Proxy Disclosure Enhancements rules in December 2009, which were effective in February 2010. These rules require disclosure of the board's role with regard to risk oversight in the company's annual proxy statement. The board's role with regard to risk oversight appears to be continually evolving.

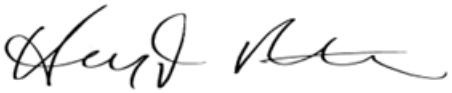
As a result of the increasing regulatory requirements for risk management oversight, Deloitte expects board risk committees to become an accepted fact of life at major banks and at many financial services companies, and, while they may not become common in other enterprises, they may be considered by large companies in virtually all industries. This guide can assist organizations of all types in developing or strengthening their risk committees. It can help the board of any enterprise, whether or not it is establishing a formal risk committee, to improve risk governance and oversight.

Therefore, we present this guide as a resource for board members and senior executives, regardless of whether they are considering (or reconsidering) their risk governance responsibilities or are actually forming, working with, or serving on a risk committee.

Although this guide is focused on risk committees of companies in the financial services industry, many of the thoughts, ideas, and recommendations provided within this guide may also be applicable to other commercial enterprises as they consider risk-oversight practices.



Maureen P. Errity, Director
Deloitte LLP
Center for Corporate Governance



Henry J. Ristuccia, Partner
Deloitte & Touche LLP and Co-Leader of
Deloitte's Governance and Risk Management services

Introduction:

Board risk committees become reality

This guide aims to assist board members of publicly held banks, BHCs, and other financial services companies — and of nonfinancial publicly held corporations — in designing, developing, and operating a board-level risk committee. Dodd-Frank[1] and the NPR will soon require such committees for certain BHCs.

Board-level separate risk committees (committees apart from the audit committee and in addition to management's risk committee, if one has been established) will be required by the NPR for bank holding companies with more than $50 billion in assets and non-bank financial companies designated as systemically important. The NPR also empowers the Federal Reserve Board of Governors (the "Board of Governors") to mandate that certain financial institutions with assets of less than $10 billion institute board-level risk committees, if the Board of Governors determines that such a committee would further encourage responsible risk management in the organization.

Deloitte developed this guide in response to growing interest in board-level risk committees as well as forthcoming rules required by Dodd-Frank. While many banks of the size required to have a board risk committee already have one, quite a few do not. Also, companies that do have board 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 given the added regulatory requirements from the passage of Dodd-Frank and those that may be required under the NPR.

Much of this guide speaks primarily to board members and risk committee members at large banks and BHCs. However, it also addresses senior executives, particularly financial, audit, and risk management executives, at those institutions. In addition, readers in other financial services companies and in commercial enterprises can improve their understanding of board-level risk committees (which are our focus here, as opposed to management risk committees). This understanding of board-level risk committees will help enable them not only to consider whether such a committee would benefit their enterprises and stakeholders, but also to consider ways to improve risk governance in their organizations in the absence of a board risk committee.

This resource guide first presents considerations for a board contemplating the formation of a risk committee (Section 1). It then covers topics that a board risk committee charter might include, hints on developing and using the charter, and describes potential qualifications of the "risk expert" that will be required by Dodd-Frank through the NPR (Section 2). Next, the guide provides suggestions related to how a board risk committee may go about fulfilling its chief responsibilities (Section 3) and educating and evaluating itself (Section 4). Each section includes example related questions to ask when developing a board risk committee, as well as tools and resources.

Although board risk committees are destined to become fixtures in U.S. banks and BHCs, they are still new relative to audit, compensation and nominating/governance committees. 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.

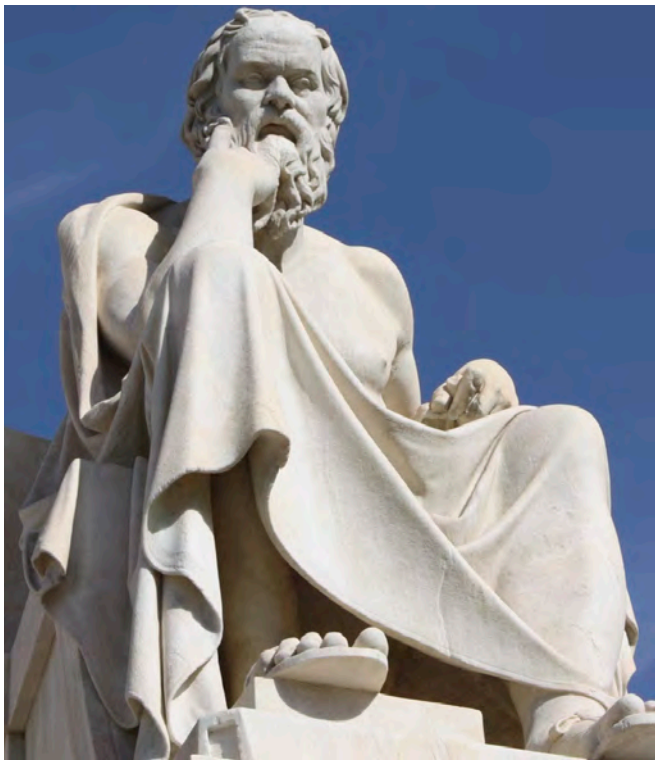
Section 1:

Considerations in forming a risk committee

While risk committees are not new for major banks, in many cases they have focused primarily on credit, market, and liquidity risks. The NPR (see sidebar on following page) may broaden those committees' responsibilities to include oversight of the entire risk management program, which includes broader risks, such as operational, reputational, and strategic risks.

Not every company — or even every bank — will need a board risk committee. However, those that consider establishing one might consider the following key factors:

- **The needs of stakeholders:** Whether or not the enterprise will be required by the NPR to have a risk committee, the needs of the enterprise and its stakeholders should be considered. It may also behoove 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 organization. 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. A related issue is whether the CRO, if there is one, will report to the risk committee, the board, or the chief executive officer (CEO) — or have a dual reporting relationship to the risk committee, or board, and the CEO. Under the NPR for banks and BHCs with more than $50 billion in assets and for non-bank financial companies designated as systemically important, the CRO will be required to report to the risk committee and CEO.
- **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 compensation 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 compensation plans might remain with the compensation 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.



The Notice of Proposed Rule Making (NPR)

Section 252.126 of the Notice of Proposed Rule Making (NPR) sets forth the following key provisions regarding the risk committee[2]:

The NPR will require: U.S. banks and bank holding companies with greater than $50 billion in assets; those with greater than $10 billion in assets and who are publicly-traded; and non-bank financial companies designated as systemically important to establish a board risk committee with a formal written charter approved by the company's board of directors.

For U.S. bank holding companies with more than $50 billion in assets and non-bank financial companies designated as systemically important, the NPR will require appointment of a CRO, who should have appropriate expertise in developing and applying risk management practices and procedures, measuring and identifying risks, and monitoring and testing risk controls commensurate with the size and complexity of the organization.

Under the proposed rules, 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:

(1) Risk limitations appropriate to each business line of the company;
(2) Appropriate policies and procedures relating to risk management governance, risk management practices, and risk control infrastructure for the enterprise as a whole;
(3) Processes and systems for identifying and reporting risks and risk-management deficiencies, including emerging risks, on an enterprise-wide basis;
(4) 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;
(5) Effective and timely implementation of corrective actions to address risk management deficiencies;
(6) Specification of management and employees' authority and independence to carry out risk management responsibilities; and
(7) Integration of risk management and control objectives in management goals and the company's compensation structure.

[2] Board of Governors of the Federal Reserve System (Board), Enhanced Prudential Standards and Early Remediation Requirements for Covered Companies; December 20, 2011; Section 252.126.

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?

For example, under New York Stock Exchange (NYSE) listing requirements, the nominating/governance committee is to "develop and recommend to the board a set of corporate governance principles applicable to the corporation; and oversee the evaluation of the board and management."[3] Under those requirements, the audit committee is to "discuss policies with respect to risk assessment and risk management."[4]

NYSE listing rules recognize that many companies assess their risk through mechanisms other than the audit committee but state that the processes "should be reviewed in a general manner by the audit committee."[5] Also, as a result of the SEC's Proxy Disclosure Enhancements rules, in addition to the disclosure requirements related to the board's role with risk oversight, companies are required to analyze compensation practices and disclose when risks arising from them are likely to have a material adverse effect on the company. The compensation committee can play an important role in overseeing that analysis and understanding how the results are disclosed.

Further, the board plays an important role in overseeing compliance and ethics programs, which may ultimately be assessed with regard to the federal sentencing guidelines. Specifically, ensuring that compliance and ethics programs are effectively established as part of a risk management program is a leading practice.

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.

[3] *Final NYSE Corporate Governance Rules*, approved by the SEC on June 30, 2003, and November 4, 2003 (http://www.nyse.com/pdfs/finalcorpgovrules.pdf)

[4] Ibid.

[5] Ibid.

Tools and resources

Deloitte's Global Risk Management Survey[6] provides a bi-annual update of the actual governance practices of more than 125 financial institutions worldwide. Now in its seventh edition, it provides an excellent view of governance in various regulatory environments while revealing points of convergence.

General guidance regarding risk governance can also be found in the Walker Review,[7] which was issued in 2009 for UK banks and financial services companies and includes useful guidelines for financial — and nonfinancial — companies elsewhere. Of the 39 recommendations in the review, numbers 23–27 focus particularly on risk committees and risk governance.

Various business and shareholder organizations have issued information regarding corporate board and committee structure and practices, including areas such as board performance, independent directors, term limits, mandatory retirement, and shareholder input in director selection. These organizations include the National Association of Corporate Directors, Business Roundtable, The Conference Board, California Public Employees Retirement System (CalPERS), and Council of Institutional Investors.

Sample questions to ask about forming a risk committee:

- Is our organization subject to the Dodd-Frank board risk committee requirement?
- Should the CRO report to the board, to the board risk committee, to management, or to both the board and management?
- Will the management risk committee report to the board risk committee, the CRO, or the CEO?
- How does the board ascertain the independence of the committee members and chair?
- How long is the term of service for members and for the chair? Will the chair position rotate, or be appointed or reappointed by the chair, vote or other means?
- What are the responsibilities of the board risk committee and of the committee chair? How will the chair, the committee, and its members be evaluated?
- 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?
- Do any of the existing board members meet the requirements to be designated as having risk management expertise as defined by the NPR?
- How will the board keep abreast of changes in regulations and in risk governance and management practices?
- How will the committee be funded, and how will the board ensure that the committee has access to the people and resources it will need to carry out its responsibilities?

[6] *Global Risk Management Survey, Seventh Edition, Navigating in a changed world*, 2011, Deloitte Global Services Limited (http://www.deloitte.com/FSIGlobalRiskSurvey)

[7] *A review of corporate governance in UK banks and other financial industry entities*, Final recommendations, November 26, 2009

Section 2:

Risk committee charter and composition

Often, the board and its risk committee define their roles in risk 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 in risk governance.

As public documents, 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 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 language that specifies:

- The separate nature of the board 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 fulfills them
- Who is responsible for oversight of *management's* risk committee, for example, whether it is the CRO, the board 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 board risk committee and the qualifications of risk committee members and the committee's risk management expert
- The board's or risk committee's responsibilities regarding the enterprise's risk appetite, risk tolerances, and utilization 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 ongoing enterprise-wide and individual-entity or line of business basis
- The risk committee's responsibility for assessing the company's actual risk appetite over time covering both banking and trading-book exposures
- The risk committee's responsibility to approve the charter of the management risk committee — if the board, in compliance with the corporate bylaws, delegates that responsibility to the risk committee
- The reporting relationships between the board risk committee and the CRO and the management risk committee
- The risk committee's oversight of management's implementation of the risk management strategy
- 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, compensation, and nominating/governance 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 maximize risk-oversight efficiency.

Tools and resources

Deloitte has developed a model board 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 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 provided to new members of the board and its committees may help onboarding and may be used in locating and hiring the committee's risk expert and other members, who may be recruited from among existing board members or elsewhere (see sidebar on the next page).
- **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.

Composition of the risk committee

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 risk committee requires independence similar to that of the audit, nominating/governance, and compensation committees — and for similar reasons. Also, as outlined in the NPR, Dodd-Frank will require certain BHCs to appoint an independent director as the chair of the committee.

Defining members' qualifications

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

Risk committee members may be recruited from its current board members; however, it may be necessary to recruit a new board member to fulfill Dodd-Frank's requirement that a "risk expert" sit on the risk committee. This guide can help the board and the nominating/governance committee to define the composition of the risk committee and the qualification of its members.

The risk expert

Section 252.126 of the NPR will require that the board risk committee "have at least one member with risk management expertise that is commensurate with the company's capital structure, risk profile, complexity, activities, size and other appropriate risk factors." Further, the NPR defines risk management expertise as follows:

(1) An understanding of risk management principles and practices with respect to BHCs or depository institutions, or, if applicable, non-bank financial companies, and the ability to assess the general application of such principles and practices;

(2) Experience developing and applying risk management practices and procedures, measuring and identifying risks, and monitoring and testing risk controls with respect to banking organizations or, if applicable, non-bank financial companies.

In addition, Deloitte offers the following observations and related suggestions:

- While the position of board risk committee risk expert is still being defined at most companies, individuals considered for the position may benefit the organization if they possess:
  - Experience as a CRO, CEO, chief financial officer (CFO), or chief compliance officer (CCO) who has successfully owned or managed a risk management program at an institution of comparable size, scope, operations, and complexity
  - Experience successfully managing significant risks — and a range of risks (for instance, beyond a single risk, such as credit or market risk) at a similar organization
  - Organizational and leadership skills required to work with committee members, the board, and management to further the cause of sound risk management in the enterprise

Questions to consider regarding a risk expert:

- What specific qualifications does the board seek in its risk expert?
- 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 organization(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 organization?
- 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 organization and what role did the individual play in developing and overseeing the risk organization?
- 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 organizational settings?
- Has this individual had the experience of identifying, analyzing, monitoring, and reporting on risk to a board of directors?
- Is this individual a good fit with the board, executive team, and major shareholders in terms of personality, team orientation, communication skills, and leadership style?

This risk expert role is somewhat analogous to the role of the financial expert required to be on the audit committee by the Sarbanes-Oxley Act of 2002. In practice, many of the requirements of the financial expert were left to the judgment of the board, and it is possible this may be the case for the risk expert as well. Note, however, that the finance and accounting profession is much more formally developed than that of risk management, given the CPA credential, the auditing process for public companies, and the broad acceptance and long tradition of CFOs. Given the developing nature of risk management and the CRO position, there is no widely accepted credential or comparatively broad talent pool from which to recruit risk experts.

Tools and resources

Deloitte continually monitors the risk-related policies and practices of large enterprises and has published the results of a number of studies, surveys, and reviews. Among the most recent are the following:

- *Risk Intelligent Proxy Disclosures – 2011: Have risk-oversight practices improved?*
- *Improving Bank Board Governance: The bank board member's guide to risk management oversight*

Asking questions and considerations related to the composition of the risk committee is one element of effective board succession and development plans. The Deloitte publication *Creating the board your company deserves: The art – and science – to choosing directors* provides useful insights on board succession and development considerations.

The risk expert role is somewhat analogous to the role of the financial expert required on the audit committee by the Sarbanes-Oxley Act of 2002.

Section 3:

Fulfilling risk-oversight responsibilities

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

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

- **Oversee the risk management infrastructure:** The full board may oversee the organization's risk management infrastructure (see sidebar), or this oversight responsibility can be delegated to the board risk committee, rather than to the audit committee (the committee that historically has had primary responsibility for overseeing the risk management infrastructure). NYSE listing requirements permit the board of a listed company to delegate this responsibility to a board-level risk committee, rather than to the audit committee.
- **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.
- **Assist with risk appetite and tolerance:** The risk committee can help establish, communicate, and monitor the risk culture, risk appetite, risk tolerances, and risk utilization of the organization at the enterprise and business-unit levels.
- **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 ongoing, 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, compensation, or other board-level committees. In cases of risks monitored by other board committees, the risk committee should be made aware of ongoing 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

The risk management infrastructure

An organization'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 board risk committee may review the risk infrastructure, or the audit committee may retain responsibility for it. 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.

full range of risks and potential interactions among risks, including risk concentrations, escalating and de-escalating risks, contingent risks, and inherent and residual risk.

- **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.
- **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 board risk committee should consider and approve the charters of any such management risk committees.
- **Oversee the CRO:** Like the chief audit executive's relationship with the audit committee, the board or its risk committee hires, evaluates, and determines the compensation of the CRO. In any case, the CRO requires direct access to the board and its risk committee, and vice versa. The management risk committee (or at least its chair) could also report to the board risk committee (or to the CRO, with a dotted line to the committee). The board and the risk committee should consider how they might maintain ongoing communication with the CRO and the risk management function, including separate sessions with the CRO.
- **Support the CRO:** The board risk committee can support the CRO by bolstering the stature of the position. In addition to having the CRO report directly to the board or the risk committee, the risk committee can help ensure that the CRO has the seniority, authority, and resources to oversee risk in the enterprise. The board can also support the CRO through consistent communications and actions (demonstrated through appropriately tailored management compensation plans) regarding the organization's approach to risk and risk management.
- **Consult external experts:** The board 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 board 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 board risk committee may seek external board education regarding risk management or regulatory matters. In other cases, the board risk committee may engage a consultant for a particular assessment or other efforts best commissioned at the board level.
- **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 organization.

The board and risk committee can assert its responsibilities in any given area by writing them into the risk committee charter. A 2011 review of board risk committee charters conducted by Deloitte among large banks and BHCs found that most of the responsibilities described above were written into some of those charters.[8]

[8] *Improving Bank Board Governance: The bank board member's guide to risk management oversight*

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.
- **Recognize IT's role:** IT is integral to risk management and oversight in every organization. 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, organizational 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 organization.

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, 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 nationalization, one upon which key manufacturing processes depend. Lack of preparation in the implementation or maintenance phases throughout an organization'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 organization. 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.

Tools and resources

Deloitte provides a number of resources to help risk committees define and fulfill their responsibilities. Many of these can be found in specific sections of Deloitte's Center for Corporate Governance website (www.corpgov.deloitte.com).

Separately, Deloitte provides in-depth resources related to the Risk Intelligent Enterprise™, which exemplifies Deloitte's approach to risk (see sidebar).

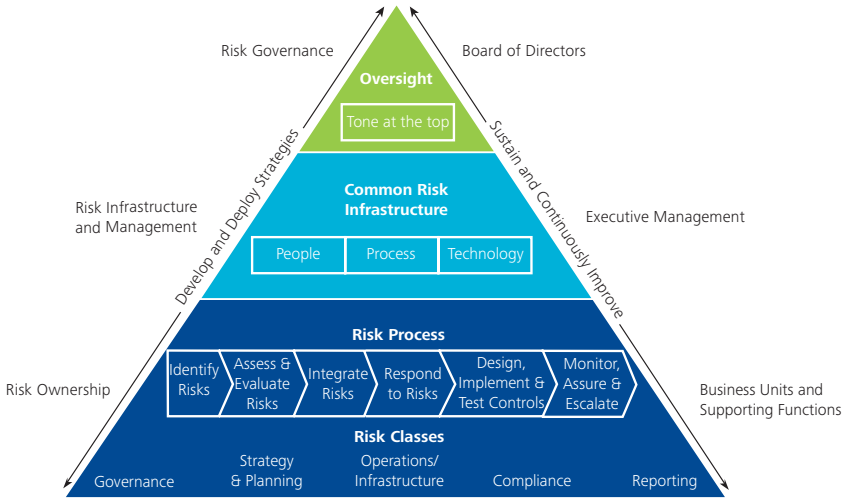
Specific resources in this area include:

- *The Risk Intelligent Enterprise™: ERM Done Right*
- *Risk Intelligent governance: A practical guide for boards*
- *Risk Intelligent Enterprise Management: Running the Risk Intelligent Enterprise*

Deloitte has also published a series of papers focused on the Risk Intelligent Enterprise™ (www.deloitte.com), a number of which are specific to certain industries (e.g., Life Sciences, Energy, Technology) or senior positions (e.g., chief audit executive, CFO, chief information officer). These papers and others in the Risk Intelligence series provide overall guidance on risk governance and management, as well as information on how specific functions, such as Internal Audit and Finance, can better address risk.

Also regarding Risk Intelligence, the framework on the right portrays the relationship between the board, the executive team, and the business units and supporting functions, and their risk-related responsibilities. The sidebar provides the nine principles of the Risk Intelligent Enterprise, which exemplifies Deloitte's philosophy of and approach to risk governance and management.

The Risk Intelligent Enterprise™ framework



Nine fundamental principles of a Risk Intelligent Enterprise

1. A common definition of risk addressing both value preservation and value creation is used consistently throughout the organization.
2. A common risk framework supported by appropriate standards is used throughout the organization to manage risks.
3. Key roles, responsibilities, and authority related to risk management are clearly defined and delineated.
4. A common risk management infrastructure is used to support the business units and functions in their risk responsibilities.
5. Governing bodies, such as board and audit committees, have appropriate transparency and visibility into the organization's risk management practices.
6. Executive management has primary responsibility for designing, implementing, and maintaining an effective risk program.
7. Business units are responsible for their business and the management of risks they take within the risk framework established by executive management.
8. Certain functions (e.g., Finance, Legal, IT, Human Resources) have a pervasive impact on the business and support the business units in the organization's risk program.
9. Certain functions (e.g., Internal Audit, Risk Management, Compliance) monitor and report on the effectiveness of an organization's risk program to governing bodies and executive management.

Other organizations have promulgated risk frameworks, as well as practices that boards and risk committees can potentially benefit from, with the Committee of Sponsoring Organizations of the Treadway Commission being the most well-known.

Risk-oversight disclosures and standards

The SEC now requires disclosure of the board's role in risk oversight. Examples of such disclosures include whether the entire board is involved, or whether risk oversight is in the purview of a specific committee, and whether key employees responsible for risk management (such as the CRO) report directly to the board. The SEC has stated that it considers risk oversight a key responsibility of the board. By requiring risk-related disclosures in proxy statements, the SEC aims to enhance investors' and shareholders' understanding of the organization's risk governance practices at the board level.

More specifically, here are 12 points that Deloitte has developed leveraging the SEC proxy disclosure requirements, which boards, risk committees, and senior management can use to help determine what may be appropriate and useful to disclose:

1. Whether the full board is responsible for risk
2. Whether the audit committee is the primary committee responsible for risk
3. Whether other board committees are involved in risk oversight
4. Whether the company has a separate board risk committee
5. Whether the compensation committee is responsible for overseeing risk in compensation plans
6. Whether the CEO is responsible for risk management or how the CEO is involved in risk
7. Whether the company has a CRO
8. The board's involvement with regard to the company's risk appetite
9. How the board is involved with regard to corporate culture
10. Whether risk oversight and management are aligned with the company's strategy
11. Whether the company has a risk committee at the management level
12. Whether the company separately addresses reputational risk

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 utilization and exposures of the organization 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 compensation committee gauged the risks that they oversee in financial reports and compensation 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 CRO and management to monitor the risk appetite and risk profile, and in a timely manner?
- Do we review and concur with the organization's disclosures regarding risks in the annual report, proxy statements, and other public documents before they are issued?

These points were developed by Deloitte based on our understanding of the SEC's amended rules on risk disclosures in proxy statements, which went into effect on February 28, 2010. For further information, including the disclosures made by Standard & Poor's companies in a range of industries in the 2011 proxy season, see the Deloitte publication *Risk Intelligent Proxy Disclosures – 2011: Have risk-oversight practices improved?*[9]

[9] *Risk Intelligent Proxy Disclosures – 2011: Have risk-oversight practices improved?*

Section 4:

Ongoing 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

NYSE listing standards require that a listed company's corporate governance guidelines address board education. As a relatively new 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.

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 proxy statements and other 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 customized 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

NYSE listing standards[10] require audit committees to perform an annual evaluation, and to include this responsibility in the audit committee charter. While this requirement does not yet apply to board risk committees, it may be advantageous to periodically evaluate the performance of the risk committee as a whole and, possibly, that of individual members.

- 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 ongoing 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 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 benefiical and appropriate.

Tools and resources

To assist risk committees in their evaluation efforts, we have included the following resources in this guide:

- Risk committee performance evaluation (Appendix C)
- Illustrated sample governance documentation (Appendix E)

[10] NYSE Corporate Governance Rule 7(b)(ii)

Conclusion:

Ever vigilant, continually improving

Much of the value of the board 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 board 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 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 prioritize 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 organization 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 recognize the risk sooner and address it more effectively already existed within the organization.

Questions to ask to encourage continual improvement in risk oversight:

- How do we evaluate not only the CRO, but candidates for 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, labor 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 characterizes sound risk governance?
- 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?

This knowledge presents board risk committees with a real opportunity. They can shoulder the responsibility of helping management to identify not only risks 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.

Tools and resources

Deloitte continues to make new tools and resources available at deloitte.com and at the Deloitte Center for Corporate Governance (www.corpgov.deloitte.com).

Appendix A:

Sample risk committee charter

This sample risk committee charter is based on leading practices observed by Deloitte in the analysis of a variety of materials. Much of the information contained herein is leveraged from two separate publications by Deloitte. First, Deloitte's Center for Corporate Governance analyzed the risk-related disclosures in the 2011 proxy statements issued by the top 200 companies in the Standard & Poor's (S&P) Index.[1] The review was based on 12 considerations most often indicated as areas of interest by board members and executives in Deloitte client interactions.[2] Second, in 2011, Deloitte analyzed 34 bank board risk committee charters.[3] Given the industry and the regulatory environment, most banks have long been addressing certain risks at the board level and thus tend to have sophisticated structures, including having a board-level risk committee from which to leverage leading practices. Given Section 165 of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank")[4], as further defined by the NPR which will require certain financial institutions to establish a board-level risk committee, the number of such committees may be on the rise. In addition to the aforementioned Deloitte publications, Deloitte analyzed other publicly available selected risk committee charters.

It is important to note that, in contrast with the Deloitte Audit Committee Resource Guide, the Risk Committee Resource Guide practices are drawn from Deloitte experiences, our understanding of practices currently being used, and the latest NPR versus mandated rules. Risk committee charter guidance has not been standardized or codified.

This template is designed for U.S. public companies; exceptions to the requirements noted below may apply for certain issuers, including investment companies, small-business issuers, and foreign private issuers. Many of the items presented here are not applicable to voluntary filers. 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 utilizing the tool.

Sample board risk committee charter

I. Purpose and authority

The risk committee is established by and among the board of directors 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 organization 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

[1] The S&P 200 listing was obtained from the top 200 companies, by revenue, in the S&P 500 index, as of March 1, 2011, from www.standardandpoors.com.

[2] *Risk Intelligent Proxy Disclosures – 2011: Have risk-oversight practices improved?*

[3] *Improving Bank Board Governance: The bank board member's guide to risk management oversight.*

[4] 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.

- 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 fulfill its responsibilities by carrying out the activities enumerated in Section III of this charter.

II. Composition and meetings[5]

The risk committee will comprise three or more directors as determined by the board. Each risk committee member will meet the applicable standards of independence, and the determination of independence will be made by the board. Each member will have an understanding of risk management expertise commensurate with the company's size, complexity and capital structure.

At least one member will qualify as a "risk expert" (required for certain financial services companies by Section 165 of Dodd-Frank, but this may be considered a leading practice guidance for other firms even if not specifically required of them). The risk committee will consider the experience of the designated member with risk management expertise, including, for example, background in risk management or oversight applicable to the size and complexity of the organizations activities, attitude toward risk, and leadership capabilities.

The risk committee will provide its members with annual continuing education opportunities and customized 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 at the annual organizational meeting of 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 nominating and corporate governance committee, may do well to consider and plan for succession of risk committee members.

The risk committee will report to the full board of directors. The risk committee will consider the appropriate reporting lines for 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.

[5] As it is critical for the risk committee to be coordinating efforts with other committees, it may make sense for the risk committee to have representation of members from the other standing board committees.

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) and even divisional CROs, the director of the internal audit function, and the independent auditor in separate executive sessions.

III. Responsibilities and duties

To fulfill 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 organization'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 organization's risk profile — its ongoing and potential exposure to risks of various types
- Define risk review activities regarding the decisions (e.g., acquisitions), initiatives (e.g., new products), and transactions and exposures (e.g., by amount) and prioritize 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 recognizes the responsibilities delegated to other committees by the board and understands that the other committees may emphasize 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 organization
- 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 summarizing 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 organization, 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 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
- 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

Chief risk officer

- Ensure that the company's CRO (if applicable) has sufficient stature, authority, and seniority within the organization and is independent from individual business units within the organization
- 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

Reporting

- Understand and approve management's definition of the risk-related reports that the committee could receive regarding the full range of risks the organization 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, proxy 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

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

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 NPR, as of December 2011. It considers the requirements for risk committees as set forth by the U.S. Securities and Exchange Commission (SEC) as well as the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank") as further clarified through the Federal Reserve's notice of proposed rule making (NPR) on enhanced prudential supervision, in addition to our understanding of common practices in the marketplace and is subject to change if additional guidance is issued. The "Results From:" section indicates if the action or responsibility results from a leading practice grounded in the NPR or our understanding of a common or emerging practice. 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 other 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 U.S. public companies; exceptions to the requirements noted below may apply for certain issuers. Many of the items presented here are not applicable to voluntary filers. All companies should consult with legal counsel regarding the applicability and implementation of the various activities identified.

	Results from			Meeting month												
Action/Responsibility	Leading practice grounded in the NPR	Common practice	Suggested frequency	January	February	March	April	May	June	July	August	September	October	November	December	Comments
Enterprise responsibilities																
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 organization'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 organization's risk profile — its ongoing and potential exposure to risks of various types		●	Continuously													

	Results from			Meeting month												
Action/Responsibility	Leading practice grounded in the NPR	Common practice	Suggested frequency	January	February	March	April	May	June	July	August	September	October	November	December	Comments
Enterprise responsibilities																
Define risk review activities regarding the decisions (e.g., acquisitions), initiatives (e.g., new products), and transactions and exposures (e.g., by amount) and prioritize them prior to being sent to the board's attention		●	Annually and as needed													
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 recognizes the responsibilities delegated to other committees by the board and understands that the other committees may emphasize 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													
Oversee the risk program/interactions with management																
Review and approve the risk management infrastructure and the critical risk management policies adopted by the organization	●	●	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 summarizing 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 organization, 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													

	Results from			Meeting month												
Action/Responsibility	Leading practice grounded in the NPR	Common practice	Suggested frequency	January	February	March	April	May	June	July	August	September	October	November	December	Comments
Oversee the risk program/interactions with management																
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 organization and is independent from individual business units within the organization	●	●	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 organization 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													

	Results from			Meeting month												
Action/Responsibility	Leading practice grounded in the NPR	Common practice	Suggested frequency	January	February	March	April	May	June	July	August	September	October	November	December	Comments
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 risk 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													

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, 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 ongoing 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 summarized 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 organization'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. Qualified risk committee members are identified by sources independent of management (e.g., independent board members assisted by an outside search firm).	0	1	2	3	4	5
2. Members of the risk committee meet all applicable independence requirements.	0	1	2	3	4	5
3. The designated risk expert meets the definition of "expert" as agreed to by the committee and the board.	0	1	2	3	4	5
4. 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
5. 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
6. The risk committee demonstrates appropriate industry knowledge and includes a diversity of experiences and backgrounds.	0	1	2	3	4	5
7. 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
8. 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
9. 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
10. The risk committee chairman is an effective leader.	0	1	2	3	4	5
11. The risk committee, in conjunction with the nominating committee (or its equivalent), creates a succession and rotation plan for risk committee members, including the risk committee chairman.	0	1	2	3	4	5
Understanding the business and associated risks						
12. 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						
13. 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
14. The risk committee considers, understands, and approves the process implemented by management to effectively identify, assess, monitor, and respond to the organization's key risks.	0	1	2	3	4	5
15. 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
16. 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						
17. The risk committee reports its proceedings and recommendations to the board after each committee meeting.	0	1	2	3	4	5
18. The risk committee develops a calendar that dedicates the appropriate time and resources needed to execute its responsibilities.	0	1	2	3	4	5
19. Risk committee meetings are conducted effectively, with sufficient time spent on significant or emerging issues.	0	1	2	3	4	5
20. 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
21. The risk committee sets clear expectations and provides feedback to the full board concerning the competency of the organization's CRO and the risk management team.	0	1	2	3	4	5
22. The risk committee has input into the succession planning process for the CRO.	0	1	2	3	4	5
23. 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
24. 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
25. Meetings are held with enough frequency to fulfill 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
26. 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
27. The risk committee maintains adequate minutes of each meeting.	0	1	2	3	4	5
28. 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
29. 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
30. The risk committee respects the line between oversight and management of risks within the organization.	0	1	2	3	4	5
31. Risk committee members come to meetings well prepared.	0	1	2	3	4	5

Circle one number for each statement	Insufficient knowledge	Strongly disagree		Neither agree nor disagree		Strongly agree
Monitoring activities						
32. 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
33. The company provides the risk committee with sufficient funding to fulfill its objectives and engage external parties for matters requiring external expertise.	0	1	2	3	4	5
Communication activities						
34. 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 organization'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 organizational 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 organization'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 utilization 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 organization – Lack of financial expertise on the audit committee	– Failure to foster an ethical culture – Inappropriate performance incentives – Failure to monitor and control unauthorized 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?

Appendix E:

Illustrated sample governance documentation

Overview

Based on Deloitte's definition of the term, a Risk Intelligent board is one in which risk is incorporated as part of every board discussion. Boards of directors that wish to become Risk Intelligent might work with management to formalize the board's risk-oversight program. A crucial step in that process is establishing a clear set of policies that define risk and the board-level responsibilities. This document includes (1) results from research performed by Deloitte in 2011 related to risk- oversight disclosures included within the proxy statement for Standard & Poor's (S&P) 200 companies and (2) suggested language that may help a board to document its roles and responsibilities related to risk oversight. The board's and its committees' corporate governance guidelines and charters, respectively, serve as the documents that outline their respective responsibilities. Including risk as part of that documentation could serve as a first step in becoming Risk Intelligent.

Listed below is an example of the primary documentation that a board may undertake to develop — the corporate governance guidelines and the committees' charters. The selected considerations under each section are meant to be indicative and not exhaustive but illustrate that it is often advantageous for boards and their committees to work together to address risk. Risks should not be siloed by committees, but rather integrated among committees. The information included herein may be used as a starting point to demonstrate how risk oversight in each of the respective documents could be applied but should be customized to the culture, organization, and the organization's risk management program and objectives. We believe that a Risk Intelligent board includes language with regard to its risk-oversight responsibilities in each of the board documents.

Analysis of risk management documentation in S&P 200

In 2010, Deloitte analyzed risk-related disclosures in proxy statements issued by S&P 500 companies. Our goal was to identify risk governance and oversight practices in light of the U.S. Securities and Exchange Commission proxy disclosure rules that went into effect on February 28, 2010. In 2011, we conducted a similar analysis, but limited to S&P 200[1] companies, in order to assess the state of disclosures and the extent of any progress, and we found evidence of steady and encouraging evolution.

In 2011, we made several modifications to sharpen the focus of the analysis. We again focused on risk governance and oversight practices at the board level, as disclosed in proxy statements filed by S&P organizations. But, rather than 20 considerations, we focused on 12 matters most often indicated as areas of interest by board members and executives in client interactions with Deloitte.

Included within this tool are excerpts of the results of 2011's analysis and identifies trends we found in risk-oversight practices at the more than 150 companies whose proxy statements we reviewed in each of the two years.

In presenting the data for 2011 on the next page (Exhibit 1), we divided the population into two primary groups, the Financial Services Industry (FSI) and others, which include: Technology, Media & Telecommunications; Consumer & Industrial Products; Healthcare Services & Government; and Energy & Resources — which we aggregate into the "All Others" category. We do this because FSI companies' risk oversight and management practices tend to be more defined in certain areas, due to the nature of their business and the risks they face. In addition, FSI risk management practices are changing rapidly as the regulatory climate evolves in light of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank"), the Basel Accords, and other regulatory developments.

[1] The S&P 200 listing was obtained from the top 200 companies, in terms of revenue, from the S&P 500 Index, as of March 1, 2011, from www.standardandpoors.com.

Exhibit 1: Benchmark finding: Deloitte's risk proxy disclosure considerations (entire sample, 2011)

Consideration	S&P 200 (170)	FSI (27)	S&P All Others[4] (143)
	% receiving a 'yes' response		
1. Does the disclosure note that the full board is responsible for risk?	90%	89%	90%
2. Is the audit committee noted as the primary committee responsible for risk?	64	48	66
3. Are other board committees noted as being involved in risk oversight?	89	78	91
4. Is the compensation committee disclosed as being responsible for overseeing risk in the compensation plans?	62	52	64
5. Does the company have a separate board risk committee?	6	33	1
6. Does the company disclose whether risk oversight/management are aligned with the company's strategy?	47	41	48
7. Does the disclosure note whether the chief executive officer (CEO) is responsible for risk management or how the CEO is involved?	35	44	34
8. Does the company have a chief risk officer (CRO)?	21	63	13
9. Does the company have a risk committee (at the management level)?	23	33	21
10. Does the disclosure note how the board is involved with regard to the company's risk appetite?	11	26	8
11. Does the disclosure note the board's oversight with regard to corporate culture?	7	19	5
12. Does the disclosure separately address reputational risk?	25	37	22

Exhibit 2: S&P 200 trend analysis: 2011 vs. 2010

Consideration	S&P 200 (2010)	S&P 200 (2011)	S&P +/– in 2011 (percentage points)
	% receiving a 'yes' response		
1. Does the disclosure note that the full board is responsible for risk?	88%	89%	+1
2. Is the audit committee noted as the primary committee responsible for risk?	65	64	-1
3. Are other board committees noted as being involved in risk oversight?	82	88	+6
4. Is the compensation committee disclosed as being responsible for overseeing risk in the compensation plans?	52	58	+6
5. Does the company have a separate board risk committee?	5	6	+1
6. Does the company disclose whether risk oversight/management are aligned with the company's strategy?	39	45	+6
7. Does the disclosure note whether the chief executive officer (CEO) is responsible for risk management or how the CEO is involved?	28	34	+6
8. Does the company have a chief risk officer (CRO)?	20	22	+2
9. Does the company have a risk committee (at the management level)?	23	25	+2
10. Does the disclosure note how the board is involved with regard to the company's risk appetite?	8	11	+3
11. Does the disclosure note the board's oversight with regard to corporate culture?	6	8	+2
12. Does the disclosure separately address reputational risk?	24	27	+3

Corporate governance guidelines

A number of stock exchanges around the world have made the documentation of corporate governance guidelines a requirement for listing. Corporate governance guidelines are intended to serve as a board-level document providing foundational practices upon which the board operates. Predominant components of many guidelines relate to director qualifications, responsibilities, compensation, orientation, continuing education, management succession, and annual board performance evaluation. Suggested below are some considerations relating to areas in which risk oversight could be documented in the board corporate governance guidelines.

Suggested considerations

- Consider the alignment of strategy with the company's views and approaches to risk-taking.
- Provide new directors with a director orientation program that will familiarize them with the company's risk management issues.
- Include continual — rather than point in time — education and monitoring of the company's key risks within directors' areas of responsibility.
- Consider defining the board's role in specifying those areas and policies where the full board expects to be consulted, including an evaluation of the associated risks (e.g., the determination of the company's earnings guidance policy and perhaps placing too much emphasis on short-term earnings).

Audit committee charter

Based on the research noted previously, it appears that the audit committee has, in many instances, become the default committee responsible for risk oversight. Of the proxy statements issued by S&P 200 companies, sixty-four percent noted the audit committee as the primary committee responsible for risk. A smaller percentage of FSI companies (versus non-FSI companies) disclose that the audit committee is primarily responsible for risk; for discussion regarding those companies that have a separate risk committee, see the risk committee charter section on page 35. The results correlate with the fact that the New York Stock Exchange has a listing requirement for audit committees to discuss policies related to financial risk assessment and risk management. However, recent events have reshaped the way companies and their boards are viewing and addressing risk throughout their organization beyond financial risk. This new and broader view of risk has resulted in boards reconsidering the need to delegate the responsibility for operational, legal, and other risks beyond the confines of the audit committee. Suggested below are some considerations relating to areas in which risk oversight is, or could be, documented in the audit committee charter.

Suggested considerations

- Clearly document the audit committee's responsibility for discussing with management the company's overall risk management policies and procedures.
- Clearly document the audit committee's responsibility for discussing with management the financial reporting exposures, which may encompass the broader financial risks of the enterprise.
- Be cognizant of the fact that the audit committee has a number of compliance responsibilities to fulfill, which may necessitate delegating the responsibility for other risks to the full board or other standing committees.
- Clearly document the scope and definition of the risks delegated to the audit committee.
- Consider the adequacy of the companies' risk disclosures.

Risk committee charter

The risk committee is one that continues to be less common outside of the Financial Services industry, which has over time established various forms of management risk committees to address the vast array of financial risks ranging from foreign currency to credit and interest rate to liquidity and general market risks.

However, Dodd-Frank through the NPR may ultimatley require: 1) U.S. banks and bank holding companies with greater than $50 billion in assets, 2) those with greater than $10 billion in assets and who are publicly-traded and 3) non-bank financial companies designated as systemically important to establish a board risk committee with a formal written charter approved by the company's board of directors and for US banks and bank holding companies with greater than $50 billion in assets and non-bank financial companies designated as systemically important, such board risk committee to not be housed within another committee, report directly to the board, and receive and review regular reports from the CRO.

Based on the analysis described above, the majority of companies operating outside of the financial services sector do not have a separate risk committee; rather, they may rely on the audit committee or all board committees to play a role in overseeing the risk management program. Recent economic events that began in the financial sector have illuminated the need to broaden perspectives on risk and the effect that interdependent risks can have on each other. To the extent a board's governance structure includes a risk committee, below is a list of considerations for this committee to weigh as it defines its chart of work. These considerations could be viewed in conjunction with the sample risk committee charter, which can be found in Appendix A.

Suggested considerations

- Consideration to the level of complexity in the organization and whether the risks can be effectively addressed by other committees of the board or whether the complexity and magnitude of risks requires a separate committee.
- As a part of defining the roles and responsibilities for risk oversight, the board could be clear about which committees are charged with performing the work to oversee specific risks.
- Regardless of structure, the board could consider the communication and coordination of efforts among the various board committees and the full board.

Compensation/remuneration committee charter

A primary responsibility of the compensation/remuneration committee is to not only review and approve the goals and objectives relevant to CEO compensation but also to evaluate the performance of the CEO in light of those goals. Based on our research, 58 percent of the S&P 200 companies evaluated in the 2011 research project disclosed the compensation committee as being responsible for overseeing the risk in the compensation plans. The recent experiences of directors relating to the global recession and the related backlash from the media, investors, and government against some CEO remuneration packages may lead to a change in their perspectives on the amount of risk associated with a company's compensation program for not only its CEO, but for the company overall. Additionally, Dodd-Frank includes provisions requiring the enhancement of proxy disclosures, one of which is related to incentive-based compensation plans that the regulators determine encourages inappropriate risks by covered financial institutions. Therefore, below are suggestions for how compensation/remuneration committees may want to document the consideration of risk-oversight responsibilities as they relate to this committee's chart of work.

Suggested considerations

- Consider risk scenarios specific to executive compensation as well as other incentive plans.
- Consider alignment of CEO pay with the overall performance goals and objectives of the organization.
- Consider incorporating scenario analysis into the proposal process and subsequent monitoring of compensation plans brought before the committee for approval.
- Consider the risks and exposures associated with employment agreement provisions, such as claw-backs or hold-to-retirement clauses.
- With regard to all compensation areas, consider the transparency of disclosures made and the risks associated with shareholder proposals.

Nominating/corporate governance committee charter

The nominating/corporate governance committee's purpose and responsibilities usually center on identifying individuals qualified to become board members, recommending nominees for approval at the next annual meeting of shareholders, developing and recommending to the board a set of corporate governance principles applicable to the corporation, and overseeing the evaluation of the board and management. Given that this committee helps to set the tone for the governance programs of an organization and influences the nomination process, this committee plays a significant role in setting the tone with regard to risk management for the organization. As a result of this notion, below are suggested considerations for inclusion in the nominating/corporate governance committee charter of work, which demonstrates how this committee might play a significant role with regard to risk oversight as it carries out its responsibilities.

Suggested considerations

- Incorporate risk management in the director-election process (e.g., evaluate the risk that board candidates lack the requisite skills for the needs of the organization).
- Consider including among the responsibilities for this committee the evaluation and assessment of the design and effectiveness of the processes in place to perform and review the organization's enterprise-wide risk assessments.

Conclusion

A clear set of roles and responsibilities that are defined for the board in its corporate governance guidelines and board committee charters is not only crucial for governance and oversight of enterprise-wide risks, but it also helps to set the tone for the organization that risk-related activities are critically important and will be monitored by the board.

Appendix F:

Illustrative considerations for a board of director's self-evaluation

Overview

Based on our knowledge, an annual self-assessment/-evaluation of board effectiveness is a leading practice and at the standing committee level is a United States stock exchange listing requirement for boards of directors. Many self-assessment questionnaires tend to focus principally on process. Questions may revolve around issues related to attendance records, preparation and distribution of the agenda, preparation of board members prior to the meeting, amount of time spent on discussion as opposed to just presentations by management, etc. One option for you, as a board member, to increase your performance level of overseeing risk management is to include within your annual self-assessment process considerations that address how well the board feels it is doing in fulfilling this oversight role. More importantly, do you feel that the board has assimilated the identification, evaluation, and discussion of risk into the overall processes of the board? Or, as we define it, has the board become "Risk Intelligent?"

This tool provides suggested topics for consideration by a board of directors for inclusion in its annual self-evaluation process. The suggested considerations under each section are meant to be indicative of suggested areas for inclusion in the self-assessment but should not be deemed exhaustive. For each section, we provide specific areas where risk oversight might be included for evaluation. The information included herein can be used as a starting point, and should be customized to the organization. We have broken the tool down into four areas, including board composition and competency, processes and policies, information and communication, and board oversight. One area that transcends all four of these is culture. It is through the culture created by you as a board member that the tone for the rest of the enterprise is defined. Establishing good fundamentals in the boardroom allows for the rest of the company to follow in the board's footsteps in their approach to ethics, integrity, risk, and the general manner in which managers and employees conduct themselves. In all areas of the assessment, consider the willingness of the directors to challenge and be challenged constructively, whether the discussions on the respective topics (noted below) include a sufficient level of candor and risk awareness and knowledge sharing, and if the board demonstrates the importance of integrity and an ethical climate, while always focusing on protecting the interests of stakeholders.

Board composition and competency

The nominating/corporate governance committee is usually charged with the duty of developing the composition and competency of the board. The nomination process should ensure that the board is comprised of directors with the right experience, knowledge, and skill set. It should also include the determination of the appropriate board size, committee structures, continuing director education, and the evaluation process for the board and its committees.

Suggested considerations

- Selection process/evaluation of board candidate credentials and references
- Alignment of board/committee capabilities with organization's markets and stage of development
- Independence as it relates to legal requirements and in the approach to serving on the board
- Diversity of board/committee expertise and backgrounds in order to compose a board that fosters Risk Intelligent decision-making
- Availability of board members to spend sufficient time fulfilling their duties
- Whether board members have sufficient knowledge and understanding of the organization's values, mission, strategy, and business plans

Processes and policies

An organization needs to be well-founded in its processes and policies, but even the most well-engineered process is still susceptible to failure. Therefore, it is important to understand that processes and policies are the starting point in creating a sound governance environment. The board could assess all of the specific processes and policies undertaken in the governance framework.

Suggested considerations

- Number and length of meetings
- Organization and management of meeting agendas
- Preparedness of board members at meetings
- Availability of board members to management outside of meetings
- Appropriate prioritization of issues for board deliberation
- Level of information provided by management in pre-meeting reading materials

Information and communication

With the overwhelming amount of information available to management and the board, it is critical to focus on providing information that is useful to the board's efforts to effectively oversee the company. This requires that management and the board continually engage in a two-way dialogue on the development of effective reporting tools and methods.

Suggested considerations

- Timely, consistent, accurate, reliable, and relevant to the right issues
- Brief and clear enough to be digestible by the board
- Responsiveness of management to requests for additional information
- Information received is appropriate and sufficiently transparent to enable a risk-focused discussion
- Availability and utilization of professional advisor views

Board oversight

The role of the board is typically a function of the legal environment in which a company operates. However, there are common responsibilities as a fiduciary that bridge the legal jurisdictions separating enterprises; the board should consider exhibiting a duty of loyalty to the corporation and exercise reasonable care in the performance of its duties.

Suggested considerations

- Board's understanding of its oversight role and its ability to distinguish such role from managing the company for all responsibilities
- Recruitment, development, and deployment of leadership throughout the organization
- Evaluation of the CEO's performance and ethics
- Effective oversight of both executives' and directors' compensation
- Board's participation in the development of the organization's risk appetite, risk tolerances, and a robust risk framework
- Sufficient involvement in setting strategy (short term, medium term, and long term), with a focus on the critical issues that can significantly alter the company's future

In summary

There are many topics that you as a board member can cover in the self-evaluation process. The above considerations can help in generating thoughts and ideas in the planning phase for a self-evaluation, which ought to be thorough, so as to achieve the potential benefits of the evaluation process. It is important to have a champion on your board to guide this process, which could be the chair of the board or another leader, such as the chair of the nominating/corporate governance committee. Select an evaluation method that is appropriate to the makeup of your board, such as (1) data driven surveys, (2) more personal one-on-one interviews by an outside third party, (3) a facilitator-led group evaluation discussion, or (4) a combination of these. The purpose of the self-evaluation is not to focus on just "checking boxes" but to assist in the identification of those areas for improvement that are most relevant for your board.

Contacts

Henry Ristuccia
U.S. Co-Leader
Governance & Risk Management
Deloitte & Touche LLP
+1 212 436 4244
hristuccia@deloitte.com

Donna Epps
U.S. Co-Leader
Governance and Risk Management
Deloitte Financial Advisory Services LLP
+1 214 840 7363
depps@deloitte.com

Maureen Errity
Director
Center for Corporate Governance
Deloitte LLP
+1 212 492 3997
merrity@deloitte.com

Scott Baret
Partner
Global Leader, Enterprise Risk Services – Financial Services Industry
Governance, Regulatory & Risk Strategies
Deloitte & Touche LLP
+1 212 436 5456
sbaret@deloitte.com

Edward Hida
Partner
Global Leader – Risk & Capital Management
Governance, Regulatory & Risk Strategies
Deloitte & Touche LLP
+1 212 436 4854
ehida@deloitte.com