Deloitte.

Risk Committee Resource Guide for Boards

Sample risk committee charter

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

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