Deloitte.

# Risk Committee Resource Guide for Boards

## Illustrated sample governance documentation

# 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.

# 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