Shaping the new financial services marketplace series

Getting Bank Governance Right
The bank board member's guide to risk management oversight

Produced by the Deloitte Center for Banking Solutions

Shaping the new financial services marketplace

A new financial services marketplace that is very different from the old is emerging from the credit crisis. The new market will be more transparent, simplified, standardized, and regulated with fewer intermediaries.

In this series, entitled *Shaping the New Financial Services Marketplace*, the Deloitte Center for Banking Solutions will examine the rules, regulations, and operating models that evolve as the industry sails uncharted waters. Specifically, these articles will focus on strategies for success in the new marketplace, different types of global regulatory systems, the gap between financial innovation and risk management, the burden on compliance as change occurs, and steps for integrating compliance risk management.

This study, based upon an analysis of bank board committee governance charters, discusses and provides approaches to how financial institutions can better define risk governance goals, responsibilities, and the scope of their board committees.

Foreword

In the wake of the credit crisis, financial institutions will face many challenges. Foremost among them will be a heightened focus on regulation and oversight, with tighter standards already being proposed in the U.S., UK and other locations. At the institutional level, boards will continue to play an active role in defining the appropriate levels of governance and accountability, in addition to examining the appropriate levels of risk.

Many financial institutions are already establishing risk committees with charters that acknowledge the risk committee's role in risk governance. But while many charters are beginning to define elements of risk governance, are they comparable to the standards set for financial governance? Furthermore, what do best practice charters look like? And how much support is there for boards in this area?

To better understand the role of boards in setting standards for risk governance, the Deloitte Center for Banking Solutions reviewed and analyzed the charters of 30 domestic and global institutions to determine the depth and usefulness of risk information conveyed. Our findings are compiled in this report with additional guidance on what risk governance charters should include and how to ensure that they will be reinforced.

In this environment, boards have a unique opportunity to establish their leadership by implementing real change to risk governance practices. We hope this report can provide valuable perspective.

Sincerely,

Don Ogilvie
Independent Chairman
Deloitte Center for Banking Solutions

August 2009

Executive summary

Governments in many countries are increasing their oversight of financial services. The U.S. Treasury has announced its proposals for regulatory reform as have the U.K. Financial Services Authority (FSA)[1] and the European Central Bank.[2] These proposals are likely to be followed by more regulations for the financial sector. The FSA's Turner Review[3] comments specifically on the important role that boards play in setting governance standards but will use the findings of the Walker report released in August 2009, to determine whether governance requirements for financial institutions should go beyond those of the Combined Code of the London Stock Exchange.[4] While the Obama administration released its financial regulatory reform plan in June 2009, it is not clear how the proposal ultimately will be implemented, nor its impact on governance standards. Similar efforts to revise financial regulation are playing out in countries around the world.

The Delaware courts have developed a framework for the board oversight of risk management[5] in a line of cases beginning with Caremark International Inc. Derivative Litigation (1996)[6] and including Stone v. Ritter (2006)[7] and other progeny.[8] These judgments emphasize a board's responsibility to have adequate risk monitoring and controls in place and its responsibility to make business decisions in good faith. More recently, Senator Charles Schumer announced his intention to introduce legislation that would change the way boards are elected and operated. Among other things, it would specifically require all corporations to appoint a special board committee to oversee risk management.[9]

How can the boards of financial institutions, particularly banks, best prepare themselves for the greater level of oversight indicated by measures such as these? What specific standards can they look to for guidance in the area of risk governance?

In this paper, we report on a Deloitte analysis of board and board committee charters of large banks. We undertook this analysis to determine the extent to which committee charters explicitly address risk governance, and whether board charters and board committee charters that outline the elements of finance governance might provide a useful model for developing a similar approach for risk governance. (In this paper, the term "risk governance" refers to the board's oversight of the risk management process.) It is quite common for a board to discharge specific, defined responsibilities to a subcommittee (e.g., audit committee); however, subcommittee structures do not relieve the board of its responsibility.

In general, finance governance at the board level is defined with far more clarity than risk governance. After the fall of Enron and other accounting scandals in 2001, the U.S. Congress enacted the Sarbanes-Oxley Act[10] (SOX), which brought sweeping change to corporate financial governance. SOX also expanded the role of board audit committees in monitoring financial reporting risks and called for the identification of financial experts within the audit committee to oversee financial reporting. The influence of SOX is now reflected in board audit committee charters.

Many auditing and accounting responsibilities are mandated and clearly defined and therefore their charters are broadly consistent across the industry. This is much less so the case for risk governance, currently an area for voluntary disclosure, where we found considerably less detail and more variability. Given this, emulating the detail of board audit committee charters constitutes a good starting point for banks to create or revisit their board risk governance charters.

Board committee charters set out the role, responsibilities, and authorities of the committee and are required for all public company standing board committees. Therefore, charters can provide an excellent opportunity to set the board committee's risk governance goals and responsibilities and to communicate them to the broader organization, regulators, and other stakeholders. Creating an effective risk governance charter thus provides a vehicle for the board to define, clarify, assert, and enforce its role in risk governance whether in the charters of audit or risk committees. Typically, risk governance is either incorporated into the charter of the board's audit committee or into the charter of a standalone board risk committee.

A risk governance charter, irrespective of where it is directed (e.g., board audit committee or board risk committee), may include and ideally define the following core elements:

- **Risk governance structure and oversight.** Define the scope and responsibility of board oversight of risk management policies and practices across the banking organization, and articulate the responsibility of the board to sanction, review, and amend management-level risk committee charters.
- **Risk appetite.** Articulate the board's role in reviewing and approving the organization's statement of risk appetite and in monitoring the actual usage of risk appetite.
- **Reporting criteria.** Define and maintain the criteria for risk reporting to the board in order to enhance transparency and to ensure that risks are being communicated upward in a manner consistent with defined thresholds.
- **Risk monitoring.** Specify the means and methods of the board to continually monitor significant risks and trends impacting the bank's risk and compliance profile. The framework has been established by *Caremark International Derivative Litigation (1996)*[11] and in *Stone v. Ritter (2006).*[12]

Lastly, boards may wish to reinforce their risk charters by requiring there be at least one "risk expert" on the board committee responsible for risk management, similar to SOX requirements for a financial expert. A process for selecting a "risk expert" may mirror aspects of the audit committee's selection of a financial expert. Beyond having a "risk expert" who is knowledgeable of key risk management issues facing the organization, it may be helpful that the entire board be knowledgeable about the organization's core businesses, which is key to effective oversight.

We confined our research of board risk-related charters to an analysis of publicly available charters and did not explore relationships between the charters and the effectiveness of risk management procedures at any of the banks. This research is grounded in the premise that board charters are one of the most visible means of achieving and demonstrating governance standards, and that boards appear to have an opportunity to establish their leadership by implementing changes to risk management practices through committee charters. Moreover, in the current environment, risk management efforts must be effective and just as importantly perceived as such. A charter can heighten the visibility of those efforts.

Level setting: the board's role in risk oversight

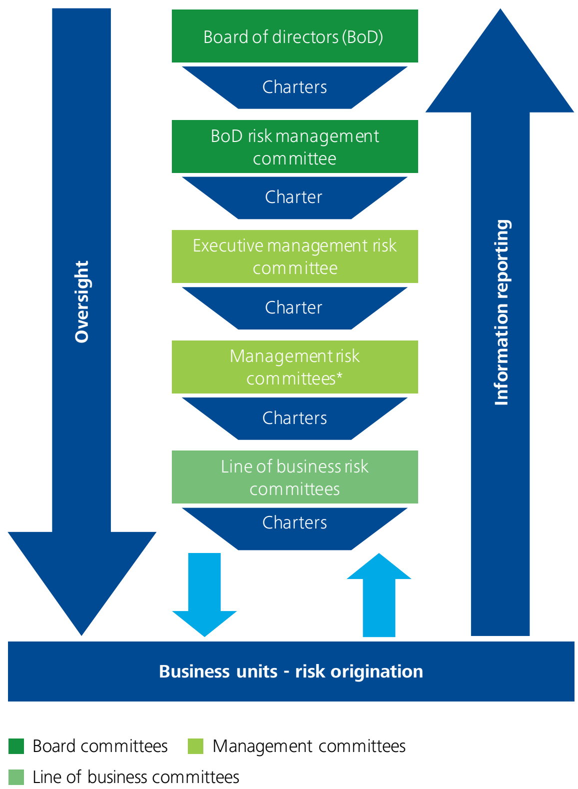
A number of boards in U.S. commercial banks have established committees with audit and risk oversight responsibilities. This does not relieve the overall board of its responsibilities, but rather allows for a more coordinated and focused approach to risk oversight. The charter of a board committee with responsibility for risk management oversight can describe the roles and responsibilities of overseeing the risk management function's policies and practices as well as the risk governance structure. The charter would do well to be consistent with and integrated into the institution's enterprise-wide approach to risk management. Final adoption of the board committee risk charter should be by the full board.

To help boards that are creating or revising risk governance charters, Deloitte has identified a number of elements of a risk intelligent governance charter. (Risk Intelligence, Deloitte's integrated approach to risk management, is addressed later in this document. Refer to Appendix A: Principles for operating a Risk Intelligent Enterprise.) By considering these elements, a board committee responsible for risk governance may better position itself to carry out its risk management oversight responsibilities.

A well-defined charter is important for three reasons. First, the charter can clearly specify risk management roles and responsibilities for the board to fulfill. Second, when posted on the company's Web site and otherwise displayed, the charter communicates to the public, regulators, and investors the organization's commitment to risk governance. Third, the charter sets the expectations for risk governance and creates a sense of accountability among all parties within the organization.

Some organizations have a number of different board and management committees, each with a distinct charter and role within the governance and risk management hierarchy. (See Exhibit 1.) The relationship among the committees, and between the committees and the board and the organization, benefits from clear definition; Exhibit 1 outlines only one possible structure.

Exhibit 1: Risk management committee oversight structure example



*Examples: Asset-Liability committee (ALCO), Credit committee, Operational risk committee, Compliance committee, etc.

Source: Deloitte research

The importance of a board designated committee responsible for risk oversight within a financial institution and the appropriateness of its composition and experience was emphasized in an October 2008 U.S. Committee of Oversight and Government Reform hearing on the collapse of Lehman Brothers. That hearing found that the organization's finance and risk management committee met only twice — in 2006 and in 2007.[13] In the transcript, the House of Representatives Committee offered the following observations on the composition of the board: "Nine are retired. Four of them are over 75 years old. One is a theater producer, another a former Navy admiral. Only two have direct experience in the financial services industry…"[14]

Elements for consideration in a risk intelligent charter

The following are important elements we recommend for consideration in risk intelligent charters:

- **Responsibility for risk governance structure and oversight.** The risk charter specifies responsibility for oversight of risk management by clearly defining the committee's scope and duties. The charter can define responsibility for the oversight of all risks relevant to the organization (both financial and non-financial risks, including market, credit, liquidity, operational, compliance, strategic, reputational, and legal). Clearly defined accountability and lines of authority across the organization's activities should be consistent with regulatory requirements and risk management policies and such alignment should reinforce the risk appetite statement.

  The charter can also articulate the committee's responsibility to sanction and review management-level risk committee charters (for example, the executive management risk committee, credit risk committee, market risk committee, and ALCO) and to approve the charters and amendments to them. The charters may be reviewed at least annually and as frequently as may be required by bank regulatory requirements. This may ensure continued consistency with the financial institution's business strategy, risk framework, risk appetite, and bank regulations.

- **Responsibility for enterprise-wide oversight of risk appetite.** The charter can articulate the committee's responsibility regarding risk appetite, that is, the institution's willingness to accept variations in results specific to a given strategy, usually expressed in a risk appetite statement. Each dimension of risk in the statement can be allocated a target level or tolerance. The statement will typically specify quantitative metrics, exposure concentrations, and similar items. It may also contain qualitative elements, such as operational risk tolerance levels and compliance standards. In reviewing the risk appetite statement, the committee might consider factors such as management's experience, the bank's strategic goals and financial strength, and the recommendations of risk management.

  In addition, tools and models used to monitor risk appetite would logically be commensurate with the complexity of the organization's business operations, finances, and reporting mechanisms. There may be a requirement for management to periodically report on key assumptions and management judgments to the board based on management's review of the assumptions underlying models and judgments used to supplement or even override such models.

- **Criteria for management's reporting about risk**. The committee may regularly discuss risk management with key senior executives and set guidelines for reporting and escalating risk issues. Furthermore, it should evaluate the frequency of formal and informal meetings with risk management committees or business executives. Scheduling formal meetings keeps risk on the organization's agenda and enables management to assess risks beforehand and to sufficiently prepare to report on risk-related matters.

- **Monitoring of risks.** The charter may specify the means and methods to continually monitor significant risks and trends impacting the organization's risk and compliance profile. It can also specify the format and content of information required and the frequency with which it should be collected and reviewed. Risk monitoring should address risk against the agreed risk appetite, encompass all material risks to the bank, and also provide transparency to risk concentrations, correlations and emerging or changing risks to the organization or a specific business.

Regulatory guidance, leading industry practices, and the current state of risk oversight

Directors are charged with fulfilling their fiduciary responsibilities to the shareholders of a company. In doing so, they are guided by regulatory requirements by local country laws, regulatory requirements, industry association guidance, securities exchange requirements, and by moral and ethical considerations. In the absence of other overriding legislation for risk governance, we can look to the general framework provided by the Bank for International Settlements (BIS) and the Office of the Comptroller of the Currency (OCC). Exhibit 2 summarizes key regulatory guidance issued by the BIS and the OCC.

Responsibilities for corporate governance for U.S. financial institutions are laid out in the proxy rules of the New York Stock Exchange, and in the following documents:

- OCC – OCC's *Manual of Examination Procedures*, in addition to the bank director guide
- OTS (Office of Thrift Supervision) - OTS 12 CFR 562.4; OTS's *Thrift Activities Handbook* and *Thrift Holding Company Handbook*
- FDIC (Federal Deposit Insurance Corporation) - FDIC 12 CFR 363 (FDICIA); FDIC's Division of Supervision *Manual of Examination Policies*
- FFIEC (Federal Financial Institution Examination Council) – Information handbooks on individual topics related to Information Technology
- Federal Reserve
  - *Bank Holding Company Examination Manual*
  - *Trading and Capital Markets Activities Manual*
  - Federal Reserve SR Letter 04-18, "Bank Holding Company Rating System," December 6, 2004 (stating that the board's involvement will factor into the overall risk and composite ratings)
  - Federal Reserve SR Letter 95-15, "Rating the Adequacy of Risk Management Processes and Internal Controls at State Member Banks and Bank Holding Companies," November 14, 1995

Exhibit 2: Board governance responsibilities

This chart reflects our interpretation of elements of the referenced guidance that we believe are relevant to board risk governance. It is not intended as a complete list, and additional elements not included here may also be important.

Regulatory Guidance	Summary of Board Risk Governance Comments
Bank for International Settlements: Basel Committee on Banking Supervision, *Enhancing Corporate Governance for Banking Organizations.*[15]	• Board members should be qualified for their positions, have a clear understanding of their role in corporate governance, and be able to exercise sound judgment about the affairs of the organization. • The board should approve and oversee the bank's strategic objectives and the communication of corporate values throughout the banking organization. • The board of directors should set/enforce clear lines of responsibility and accountability throughout the organization. • The board should ensure that there is appropriate oversight by senior management consistent with board policy. • The board and senior management should understand and effectively leverage the work conducted by the internal audit function, external auditors, and internal control functions. • The board should ensure that compensation policies and practices are consistent with the bank's corporate culture, long-term objectives and strategy, and controls environment. • The bank should be governed in a transparent manner. • The board and senior management should understand the organization's operational structure, including where the bank operates in different jurisdictions.
Office of the Comptroller of the Currency: *The Role of a National Bank Director, The Director's Book*[16]	• The board sets the overall tone and attention of the organization and establishes guidelines on the nature and amount of risk the bank may take. • One of the board's fundamental responsibilities is to select and retain competent management. • The board should ensure that bank management adequately identifies the risks associated with particular activities and has put systems and controls in place to manage that risk. • Board committees typically ensure that management has implemented accurate and reliable risk measurement systems, timely and meaningful risk reporting processes, and effective risk controls, such as policy limits, authorizations, and product approvals. • The board should identify what information and reports it wants to see from management and with what frequency. When overseeing the bank's business performance, it is often useful for the board to use peer group comparisons. The quarterly *Uniform Bank Performance Report* (UBPR), which is derived from call report data and is provided to each national bank, gives the board such a basis of comparison. • The board must make certain that the organization's liquidity and interest rate risk positions are reasonable and do not compromise the bank's ability to maintain earnings and protect capital. • The board should be certain that it fully understands the risks presented by any proposed new product or service. • When evaluating the organization's capital position, the board should be aware of the nature and extent of all balance sheet items, especially items that may require funding. • The board should oversee the management of the loan portfolio to control risks and maintain profitable lending operations. • When framing the bank's risk tolerances, directors should determine the maximum amount of organization earnings and capital they are willing to place at risk.

Analysis of board committee charters: key findings

Deloitte conducted an analysis of 25[17] U.S. headquartered commercial banks and a sample of five large non-U.S. headquartered banks by gathering and reviewing publicly available information. This analysis sought to ascertain where boards of directors at financial institutions have placed responsibility for risk management governance and oversight as of quarter end, March 31, 2009. This included noting the committee structures the boards currently employed.

More specifically, we sought to identify which charters include any or all of the important elements of a risk governance charter cited in this paper. For comparative purposes, our analysis also included a review of changes in charters that occurred between December 31, 2008 to March 31, 2009. We have noted key changes in charters in cases where they occurred.

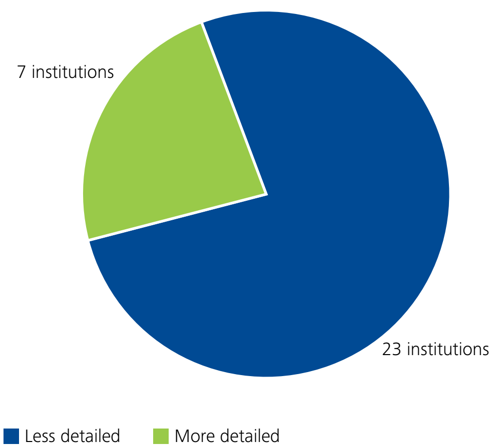
Below are our key findings regarding board risk responsibilities and the committee structures that boards employ to support risk governance.

Board risk management responsibilities – well-defined charters can provide clarity

Audit and finance responsibilities appear much more clearly and completely defined than risk management responsibilities. This was not surprising given the disclosures mandated by SOX and the voluntary requirements for disclosures for risk management committee charters. Our comparative analysis of changes from December 31, 2008 to March 31, 2009 indicates that there was a very small increase in the definition of risk management oversight in charters during this period.

None of the charters conveyed the scope and detail on risk oversight responsibilities that they did on audit responsibilities. Only seven of the 30 charters defined risk governance in detail, while the remainder had much less detail; as of December 31, 2008, the comparable statistic was six of 30. Only six of the 30 charters listed funding and liquidity risk among their oversight responsibilities; as of December 31, 2008 the comparable statistic was four of 30. As many as 10 of the 30 charters focused almost exclusively on audit responsibilities, with limited mention of risk oversight. Few of the charters covered compliance management responsibilities in detail. (See Exhibit 3.)

Exhibit 3: More detailed versus less detailed risk charters



Source: Company Web sites; Deloitte Center for Banking Solutions

The main findings of our research are listed below. (A more detailed summary of our findings is provided in Appendix B for U.S. headquartered institutions and Appendix C for non-U.S. headquartered institutions.)

- **Responsibility for risk governance.** Reflecting the fact that this is an area for voluntary disclosure, the charters we analyzed generally did not define the role of the board itself in risk management oversight in great detail. In our view, explicitly defining the role of the board in risk governance constitutes an opportunity for greater clarity. Refer to Appendix B and C for bank charters reviewed and a summary of charter information.

- **Responsibility for enterprise-wide risk appetite.** More than half of the charters included explicit language regarding risk governance responsibility and the approach for interactions and communication between management and the risk committee. However, few documented specific responsibilities regarding oversight for risk appetite.

- **Responsibility for oversight of executive risk management committees.** Only six of the 30 charters we reviewed task the board risk management committees with defined responsibilities; the comparable statistic as of December 31, 2008 was five of 30. In these cases, there were separate board risk committees and they had the most clearly defined risk governance among the charters we analyzed. Yet this group also displayed major differences in detail, suggesting the absence of a consistent approach. These results echo those of a survey conducted by the National Association of Corporate Directors revealing that 67 percent of companies assign the majority of risk-related tasks to the audit committee.[18] The survey report recommends that the board may want to consider assigning oversight of risks to certain committees to help ensure adequate coverage.[19]

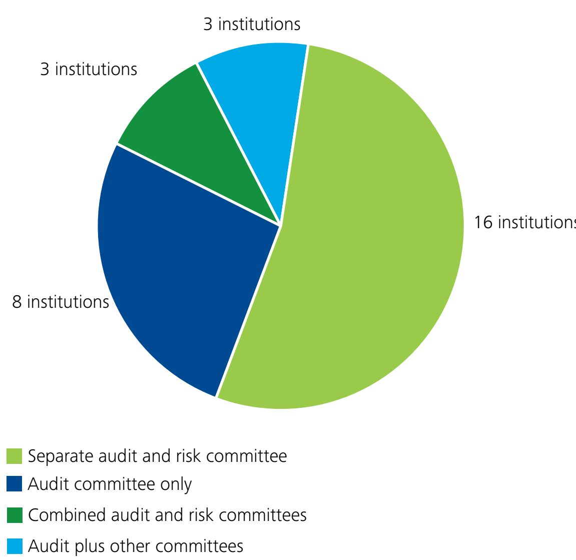
- **Responsibility for establishing the criteria for management's reporting to the board.** While some of the charters emphasize the need for management to report to the board on risk management issues, few identify the criteria under which that reporting should take place. Some charters call for regular reporting without specifying a time frame, while others refer to quarterly reporting, which may be effective in a less risk-sensitive environment.

- **Documentation of board risk management qualifications.** None of the charters explicitly required that a board member have relevant experience in risk management. Some of the charters we reviewed required an individual on the board to be designated a financial expert and to sit on the audit committee, in line with SOX requirements. A process for selecting a risk expert may mirror aspects of that for selecting the audit committee financial expert.

Committee structure – consider establishing a separate risk committee

The committee structure appears to play a role in the extent to which risk governance responsibilities are outlined. Across the various banks the responsibilities of each type of committee appeared to differ significantly. For example, 16 of the 30 banks had separate audit and risk committees, and an additional three banks had combined audit and risk committees. As one might imagine, the banks with the most well-defined risk governance responsibilities had separate risk committees. The bank boards that combined audit and risk oversight responsibilities had charters that focused primarily on their audit rather than their risk responsibilities. (See Exhibit 4.)

Exhibit 4: Committee structures outlined in charters – 30 commercial banks



Source: Company Web sites; Deloitte Center for Banking Solutions

Strengthening the role of the board in risk governance

Based on our findings, many banks have an opportunity to strengthen board charters and more clearly define the role of boards in risk governance. Appendices A and B summarize key elements of the charters reviewed. Given increasing regulatory oversight, boards have an opportunity to assess their role in risk management oversight with an emphasis on two key steps.

First, boards may wish to confirm that risk management oversight and expertise is specifically represented at the board level. Since a good percentage of bank charters in our sample did not explicitly address risk management, there is clearly an opportunity to clarify this in more detail.

Second, boards can evaluate whether responsibility for risk management oversight should rest with the full board or a board committee. The size and complexity of the bank's operations, the board members' expertise in risk management, and the number of existing board committees might also be considered. Deloitte recommends considering the establishment of a board risk management committee, separate from the audit and other committees. As our analysis suggests, separate risk committees are more likely to have well-defined risk management mandates and a stronger focus on risk-related responsibilities than committees with multiple responsibilities.

In addition, boards that decide to establish a risk committee and develop a risk committee charter may benefit by taking the following steps:

- Review Deloitte's recommended elements of a board risk committee charter and analyze the charter to determine whether the substance of those elements is present.
- Determine whether the organization's overall risk management policy accurately reflects the risk-related roles and responsibilities of the board and whether those roles and responsibilities have been reviewed and approved.
- Ensure that the risk-related responsibilities outlined in any risk committee charter can be executed given the organization's expertise and resources. If they cannot, then either the responsibilities or the resources may be adjusted accordingly.
- Analyze current board practices against guidelines issued by regulatory bodies such as the BIS and OCC, as noted in Exhibit 2, and consider the following steps:
  - Evaluate the board risk committee's experience and understanding of risk management issues, for instance the risk information it receives on limits, exposure, and new products – and what it does with that information.
  - Assess the authority that the board risk committee has delegated to management-level risk committees to manage and report on risk and to escalate issues in a timely manner.
  - Determine whether risk management policies and procedures provide sufficient risk governance and oversight as well as processes for managing each type of risk.
  - Define a transparent process for periodic, independent assessments of the board risk committee's governance, risk management, and compliance activities.
  - Establish means of formal and informal communication between the board and risk management committees.
- Analyze current board composition and consider the addition of a board-level "risk expert." Boards may wish to reinforce their charters by requiring at least one "risk expert" on the board and more importantly on the committee responsible for risk management. Some boards have recently recognized the importance of risk expertise in their recruitment of board members. In such cases, the charter can specify a general requirement for committee members to be knowledgeable about risk and relevant financial products. More broadly, the entire board's knowledge of the company's core businesses is key to effective oversight. Regarding the risk expert role, while there are likely to be less objective criteria for a risk expert than for a financial expert in a SOX context, it is certainly possible to define such criteria, which may include the following:
  - An employment background that indicates the required experience and understanding of the organization's business activities and their risk implications.
  - Sufficient knowledge of key regulatory requirements facing the organization.
  - A familiarity with risk management activities and committee functions.
  - An understanding of risk reporting metrics and information and the ability to assess the requirements of an enterprise risk management program commensurate with the organization's needs.
  - A record of success in leading a risk management program comparable to that of the organization.

A risk intelligence maturity model for governance

In the current environment, banks must demonstrate the highest standards of effectiveness, efficiency, accountability, and transparency in risk governance and management. The current state of some of the bank charters that we reviewed point to several areas for potential improvement. In reviewing their charters and defining their approach to risk governance, boards may find useful guidance in a risk intelligence maturity model. (See Exhibit 5.) This model can supplement the boards' current efforts to define the desired level of oversight both now and in the future.

Deloitte's risk intelligence maturity model has been built based on our nine principles of a risk intelligence enterprise. Below is an illustrative example of our maturity model highlighting risk governance roles and responsibilities.[20]

Exhibit 5: Risk intelligence maturity model – risk governance roles and responsibilities

				Risk Intelligence Maturity Model				
Principles for Building a Risk Intelligent Enterprise	Primary Owner	Responsibility	Key Duty	1. Unaware	2. Fragmented	3. Top-Down	4. Systematic	5. Risk Intelligent
Key roles, responsibilities and authorities relating to risk management are clearly delineated within the organization	Board of Directors	Risk Governance	Discharge risk management responsibilty for oversight	The board has not established the necessary oversight essential for influencing risk management and establishing a culture of risk awareness throughout the enterprise.	The board has established oversight, but it is not widely adopted nor well understood. Consequently, the management of risks and the culture of risk awareness only exists separately and unevenly within individual lines of business and not across the enterprise.	The board has established oversight and it has been clearly communicated throughout the organization. As a result, management demonstrates a culture of risk awareness, but risk management disciplines have not been embraced broadly or evenly across the enterprise.	The board has established oversight that is widely understood and adopted, creating a culture of risk awareness and the adoption of risk management disciplines throughout the enterprise.	The board has established oversight and is constantly seeking ways to influence the improvement of the culture of risk awareness and the management of risk throughout the enterprise to further the firm's market leadership.

The board provides an important role in risk management by providing oversight to the risk management function, by working collaboratively with management in setting the tone for risk management, and helping make sure that management sets the right objectives in the risk management program.

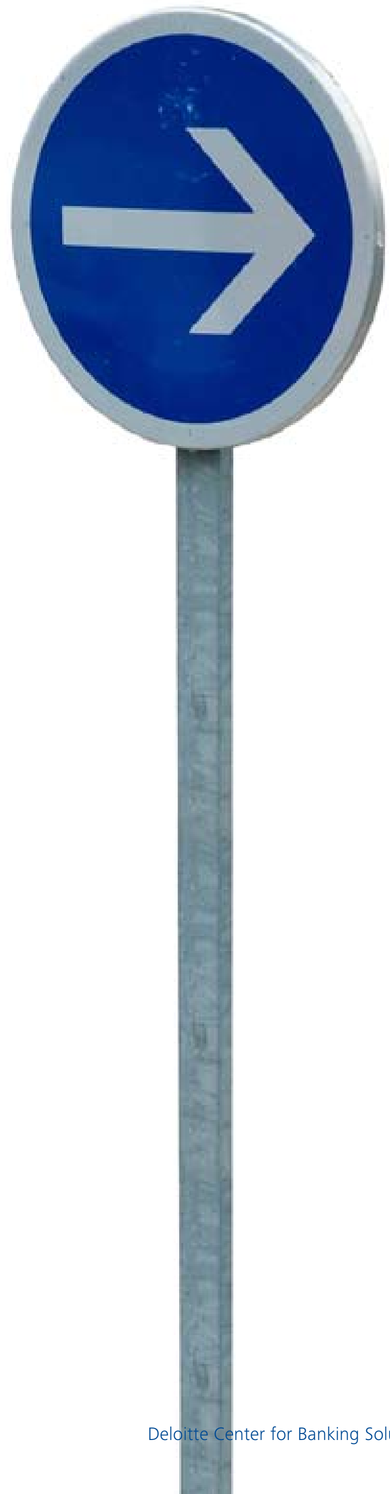
Source: Deloitte Risk Intelligence

Conclusion

In light of a tighter regulatory environment, boards have an increasingly important role to play in risk governance. Not only must they play a more active role, they must also be seen as doing so. This is particularly important for banks that have the government as a shareholder or provider of funding. One way to define the role of boards is through charters that specify risk-related responsibilities and the board's philosophy of and its involvement in risk governance.

Based on our benchmarking research, there appears to be considerable opportunity for banks to enhance their risk committee charters and for boards to employ such charters to exercise risk governance.

While the chief executive officer is responsible for risk management and the chief risk officer is responsible for running the risk management function, the board is responsible for exercising oversight regarding risk management. The recommendations outlined in this paper are intended to help board members assess their current state and plan for the future, and the principles for operating a Risk Intelligent Enterprise can provide some important perspective on these tasks (See Appendix A.)

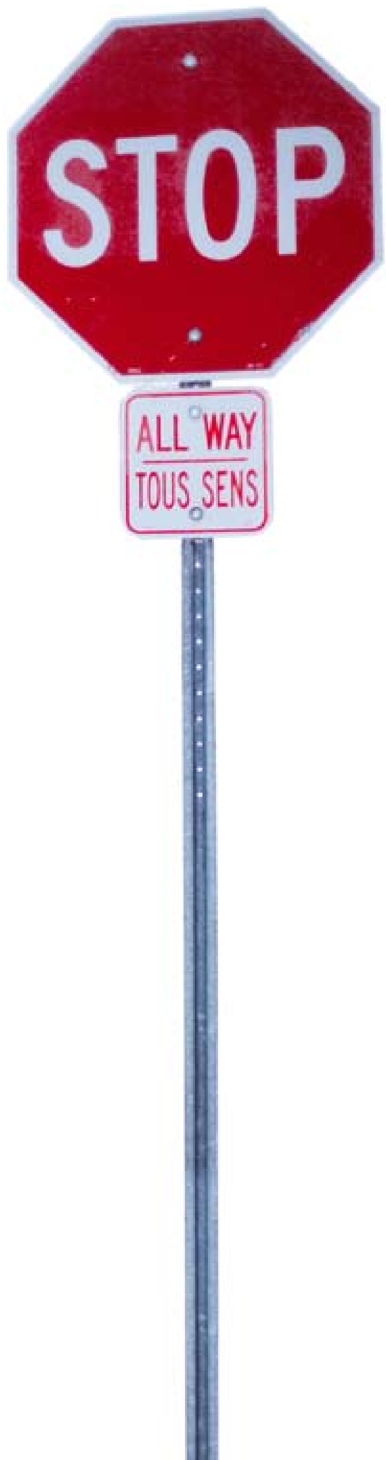


Appendix A

Principles for operating a Risk Intelligent Enterprise

In our view, Risk Intelligent Enterprises adopt a balanced perspective of risk management, supported by the following fundamental principles:

1. A common definition of risk, which addresses 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 relating to risk management are clearly defined and delineated within the organization.
4. A common risk management infrastructure is used to support the business units and functions in the performance of their risk responsibilities.
5. Governing bodies (e.g., boards, audit committees, etc.) have appropriate transparency and visibility into the organization's risk management practices to discharge their responsibilities.
6. Executive management is charged with primary responsibility for designing, implementing, and maintaining an effective risk program.
7. Business units (departments, agencies, etc.) are responsible for the performance of their business and the management of risks they take within the risk framework established by executive management.
8. Certain functions (e.g., finance, legal, IT, HR, etc.) have a pervasive impact on the business and provide support to the business units as it relates to the organization's risk program.
9. Certain functions (e.g., internal audit, risk management, compliance, etc.) provide objective assurance as well as monitor and report on the effectiveness of an organization's risk program to governing bodies and executive management.



Appendix B

Summary of bank committee charters

U.S. headquartered banks - high level summary

U.S. headquartered bank	Identified risk related committees as of March 31, 2009	Summarization of committees addressing risk management
Bank A	• Asset quality committee • Audit committee	**Asset quality committee** covers credit and market risk as required by the Basel II Accord or other regulatory requirements. **Audit committee** discusses with management the results of examination activities of corporate audit and credit review staffs, and performance thereof, including policies with respect to risk assessment and risk management.
Bank B	• Audit committee • Risk committee	**Audit committee** will review and discuss policies with respect to risk assessment and risk management. **Risk committee** covers significant financial and other risk exposures and the steps management has taken to monitor, control and report such exposures, including, without limitation, credit, market, fiduciary, liquidity, reputational, operational, fraud, strategic, technology, data-security and business-continuity risks.
Bank C	• Executive and risk management committee • Audit committee	**Executive and risk management committee** covers the processes for identifying, assessing, monitoring and managing credit risk, liquidity risk, market risk, operational risk, reputational risk and business strategy risk. **Audit committee** discusses with management, the general auditor, and the independent auditor the major financial risks and exposures and the steps management has taken to monitor, minimize or control such risks or exposures, including the company's risk assessment and risk management policies.
Bank D	• Audit and risk committee	**Audit and risk committee** covering audit and risk management duties. Risk management duties cover policies, procedures, risk parameters and organization exposures.
Bank E	• Audit and risk management committee	**Audit and risk management committee** covering audit and risk management. Duties cover oversight for the policy standards and guidelines for risk assessment (credit, market, liquidity, operational, and regulatory risk) risk management, including review of management's policies and personnel.
Bank F	• Audit committee • Enterprise risk committee	**Audit committee** provides assistance to the board by overseeing the integrity of the corporation's financial statements as well as the corporation's compliance with legal and regulatory requirements, including the performance of the corporation's internal audit function and outside auditors. **Enterprise risk committee** assists the board in promoting the best interests of the corporation by overseeing policies, procedures and practices relating to enterprise-wide risk and compliance with bank regulatory obligations.
Bank G	• Risk and compliance committee	**Risk and compliance committee** ensures that the bank is taking appropriate measures to identify, assess, monitor, control and mitigate the bank's risks in the areas of asset and liability management, credit, market, operations (including new products), technology and acquisition integration. Duties include developing and maintaining policy, and reviewing risk indicators.
Bank H	• Audit committee • Risk policy committee	**Audit committee** takes into consideration the board's allocation of responsibility for review of credit risk, market risk and fiduciary risk to the board's risk policy committee, discuss with management guidelines and policies for assessing and managing the corporation's exposure to risks, including reputation risk, the corporation's major financial risk exposures and the steps management has taken to monitor and control such exposures. **Risk policy committee** is responsible for oversight of the CEO's and senior management's responsibilities to assess and manage the corporation's credit risk, market risk, interest rate risk, investment risk, liquidity risk and reputational risk, and is also responsible for review of the corporation's fiduciary and asset management activities.

Summary of bank committee charters

U.S. headquartered banks - high level summary

U.S. headquartered bank	Identified risk related committees as of March 31, 2009	Summarization of committees addressing risk management
Bank I	• Audit committee • Risk management committee	**Audit committee** reviews with the chief risk officer or designee, any material reports or inquiries received and policies with respect to risk assessment and risk management. **Risk management committee** covers the review and oversight of the corporation's policies, strategies and activities relating to the management of credit, market, interest rate, liquidity and funding risks, including, as appropriate, audit and/or risk reviews performed in these same risk areas. Operational risk covered by the audit committee.
Bank J	• Audit and risk committee	**Audit and risk committee** covers the corporation's major financial risk exposures and the steps management has taken to monitor and control such exposures, including the bank's risk assessment and risk management policies.
Bank K	• Audit committee	Risk charters could not be located on the company's Web site. **Audit committee** charter does not specifically document risk related duties and responsibilities.
Bank L	• Audit committee • Risk and public policy committee	**Audit committee** inquires of management, the general auditor, and the independent registered public accounting firm about significant risks or exposures and discusses guidelines and policies to govern the steps management has taken to minimize such risk. **Risk and public policy committee** covers review and approval of risk assessment and risk management policies and procedures, and related risk activities, including limits and limit allocations for credit risk, market risk, interest rate risk, liquidity risk, and operating risk.
Bank M	• Audit committee	Risk charters could not be located on the company's Web site. **Audit committee** charter does not specifically document risk related duties and responsibilities.
Bank N	• Audit committee	**Audit committee** covers discussion generally with the corporation's chief risk officer of the corporation's enterprise-wide risk structure and related processes, guidelines, and policies.
Bank O	• Audit committee	**Audit committee** briefly mentions the duty to inquire about significant risks and exposures, if any, and the steps taken to monitor and minimize such risks.
Bank P	• Audit committee	**Audit committee** covers discussions with management regarding the company's major financial risk exposures and the steps management has taken to monitor and control such exposures, including the company's risk assessment and risk management policies.
Bank Q	• Executive committee • Examining and audit committee	**Executive committee** reviews and discusses with management the corporation's assessment and management of risk, including operational, interest rate, liquidity, credit and trading risks, and related policies. The committee is also responsible for discharging the duties and obligations of the board of directors under Basel II. **Examining and audit committee** discusses guidelines and policies that govern the process by which risk assessment and risk management is handled by the corporation. The committee's oversight responsibility in this regard shall recognize the role of the executive committee, delegated by the board, concerning the corporation's risk assessment and risk management. Therefore, this oversight responsibility shall consist of a general review of the activities of the executive committee regarding risk assessment and risk management guidelines and policies.
Bank R	• Audit committee • Risk committee	**Audit committee** meets with management to review the company's major financial reporting risk exposures and the steps management has taken to monitor and control such exposures, including the company's risk assessment and risk management policies. Additionally, it coordinates with the risk committee the exchange of information and reports regarding the activities of both committees, as necessary and appropriate. **Risk committee,** at least annually, reviews and approves the charters of the corporate asset/liability management committee ("ALCO"), credit management committee, operational risk committee, and the enterprise risk committee. The committee shall also review and approve the company's significant risk assessment and risk management policies. In addition, the committee retains the ability to authorize management to develop and implement any additional policies relating to risk assessment and risk management.

Summary of bank committee charters

U.S. headquartered banks - high level summary

U.S. headquartered bank	Identified risk related committees as of March 31, 2009	Summarization of committees addressing risk management
Bank S	• Audit committee • Finance and capital committee • Risk management committee	**Audit committee** oversees the integrity of the company's financial reporting process, business risk assessment, compliance with applicable laws and regulations and the adequacy of underlying internal controls. **Finance and capital committee** covers policy regarding internal financial performance metrics including risk-adjusted returns on economic capital, overall financial plans and projections, including plans for significant business units and key assumptions and risk factors inherent in such plans and the liquidity and market rate risk of the bank's on-and off-balance sheet assets and liabilities; sensitivity of earnings to changes in interest; hedging strategies and related policies concerning the use of derivative instruments to manage these risks. **Risk management committee** shall cover how to effectively and efficiently monitor the evolution of the company's risk management process, especially focusing on new and emerging risks.
Bank T	• Audit committee • Risk management committee	**Audit committee** covers discussions with management and the independent auditors, the company's guidelines and policies with respect to risk assessment and risk management, major financial risk exposures and the steps management has taken to monitor and control such exposures. **Risk management committee** in exercising its oversight role of financial, liquidity, market and operational risks, the committee is entitled to rely on management to assume the primary risk management function, including the responsibility to establish appropriate policies, practices and procedures.
Bank U	• Audit committee • Risk committee	**Audit committee** covers policies and guidelines for assessing and managing the corporation's exposure to any significant risks, including any steps taken by management to monitor, minimize or control the corporation's exposure to risks, including major financial risk. **Risk committee** covers the review and approval of the charter of the senior risk committee, asset and liability committee, credit risk committee, market risk committee, operational risk committee, and conflict review committee. The committee shall also review and annually approve the corporation's risk policy, and annually review the corporation's risk management governance overview, liquidity and interest rate sensitivity risk policy, market risk policy, credit risk policy, and operational risk policy.
Bank V	• Audit committee • Finance committee	**Audit committee** consults with chief legal officer and chief risk officer concerning legal and regulatory matters. **Finance committee** approves and monitors the administration of, policies (the "Finance Policies") that govern the company's financial risk management, such as activities related to capital, funds, liquidity, interest rate risk and credit risk management.
Bank W	• Audit and examination committee • Credit committee	**Audit and examination committee** along with the head of compliance and enterprise risk management group provide at least quarterly reviews of the enterprise-wide compliance risk management program. **Credit committee** reviews the quality of the company's credit portfolio and the trends affecting that portfolio to: oversee the effectiveness and administration of credit-related policies; review the adequacy of the allowance for credit losses; and provide oversight and guidance to the board regarding the credit-related aspects of implementing the Basel II Capital Accord.
Bank X	• Audit committee • Credit committee	**Audit committee** discusses with management, the independent auditors and the director of internal audit (i) the guidelines and policies governing the process by which senior management of the company and the relevant departments of the company assess and manage the company's exposure to risk and (ii) any significant financial risk exposures and what steps management has taken to monitor, control and report on such exposures. **Credit committee** monitors the results of internal credit reports and examinations and examinations by bank regulatory authorities and outside auditors, and review, evaluate and recommend changes to policies established by the board and by management.
Bank Y	• Audit committee	**Audit committee** responsibilities relating to retention of public accounting firms, review of financial statements and disclosures, appointment of auditors, oversight of the company's internal audit function,and compliance oversight function.

Source: Deloitte analysis of individual bank charters as provided on bank Web sites as of March 31, 2009

Appendix C

Summary of bank committee charters

N0n-U.S. headquartered banks - high level summary

Non-U.S. headquartered bank	Identified risk related committees as of March 31, 2009	Summarization of committees addressing risk management
Bank AA	• Audit committee • Risk committee	**Audit committee** reviews the report that identifies high-level control issues of group level significance that require, or are subject to, remedial attention and summarizes the actions being taken to resolve those issues. This report is compiled on behalf of the group executive committee by the bank's risk group in conjunction with the bank's internal audit, legal, the external auditors and based on issues raised by the group's governance and control committees. **Risk committee** is responsible for activities such as risk framework, governance, firm appetite and profile, policies, and receiving and reviewing risk reports.
Bank BB	• Audit committee • Risk committee	**Audit committee** charter was not located. Corporate governance report from 2007 was able to provide a brief summary of committee structure and responsibilities. There was no specific reference to risk related responsibilities. **Risk committee** meetings have the management board reports on credit, market, liquidity, operational, litigation and reputational risks. Chief Risk Officer is a member of the management board.
Bank CC	• Group audit committee	**Group audit committee** covers group-wide consolidated risk and control assessment.
Bank DD	• Corporate risk management committee • Internal audit and compliance committee	**Corporate risk management committee** covers the basic policy of the corporate risk management for the entire group. Each group company will organize its own administrative system and manage risks. These group companies will report various analysis of risk to the committee and the executive committees. **Internal audit and compliance committee** is comprised of outside directors and specialists, deliberates important matters relating to internal audits, internal control of financial information, financial audits, compliance, corporate risk management, and other internal control systems.
Bank EE	• Risk committee • Group executive board (GEB)	**Risk committee** approves the risk authorities and the principal risk control standards, concepts, methodologies and limits within the group risk principles, capacity and exposure, as they have been defined by the board. It defines the level of authority to be delegated to the GEB. The chairman's office acts as risk committee of the board. Note in the most recent 6K (Q1 2008 report filed with the SEC): "The Board of Directors (BoD) has initiated a re-organization of its structure that includes allocating the functions of the chairman's office - which will no longer exist - to a number of new BoD committees, each of which have a majority of independent directors. This will include a newly established risk committee." **Group executive board** has overall responsibility for implementing the risk management and control principles, for approving the core risk policies as proposed by the group chief risk officer and for managing the risk profile of the bank as a whole.

Source: Deloitte analysis of individual bank charters as provided on bank Web sites as of March 31, 2009

Authors

A. Scott Baret
Partner
Deloitte & Touche LLP
sbaret@deloitte.com
+1 212 436 5456

David Cox
Director
Deloitte Services LP
dcox@deloitte.com
+1 212 436 5805

Edward T. Hida II, CFA
Global Leader - Risk & Capital Management
Partner
Deloitte & Touche LLP
ehida@deloitte.com
+1 212 436 4854

Industry Leadership

Jim Reichbach
Vice Chairman
U.S. Financial Services
Deloitte LLP
jreichbach@deloitte.com
+1 212 436 5730

Contributors

Prashant Masand
Manager
Deloitte & Touche LLP
pmasand@deloitte.com
+1 617 437 3437

Christopher Smith
Manager
Deloitte & Touche LLP
christsmith@deloitte.com
+1 617 437 3715

Deloitte Center for Banking Solutions

Don Ogilvie
Independent Chairman
Deloitte Center for Banking Solutions
dogilvie@deloitte.com

About the Center

The Deloitte Center for Banking Solutions provides insight and strategies to solve complex issues that affect the competitiveness of banks operating in the United States. These issues are often not resolved in day-to-day commercial transactions. They require multidimensional solutions from a combination of business disciplines to provide actionable strategies that will dramatically alter business performance. The Center focuses on three core themes: public policy, operational excellence, and growth.

To learn more about the Deloitte Center for Banking Solutions, its projects and events, please visit www.deloitte.com/us/bankingsolutions. To receive publications produced by the Center, click on "Complimentary Subscriptions."

Endnotes

1 *"The Turner Review – A Regulatory Response to the Banking Crisis,"* Financial Services Authority, March 2009.
2 *The High-Level Group on Financial Supervision in the EU*, ECB, February, 2009.
3 *"The Turner Review – A Regulatory Response to the Banking Crisis,"* Financial Services Authority, March 2009.
4 Responsibilities for corporate governance for U.S. financial institutions are laid out in the proxy rules of the New York Stock Exchange; the oversight responsibility of directors was further reinforced by the Caremark decision and other decisions, and in the following documents:
  a) OCC – OCC's *Manual of Examination Procedures*, in addition to the bank director guide
  b) OTS - OTS 12 CFR 562.4; OTS' *Thrift Activities Handbook* and *Thrift Holding Company Handbook*
  c) FDIC - FDIC 12 CFR 363 (FDICIA); FDIC's *Division of Supervision Manual of Examination Policies*
  d) FFIEC – Information handbooks on individual Information Technology related topics
  e) Federal Reserve
    a. *Bank Holding Company Examination Manual*
    b. Trading and Capital Markets Activities Manual
    c. Federal Reserve SR Letter 04-18, "Banking Holding Company Rating System," December 6, 2004 (stating that the board's involvement will factor into the overall risk and composite ratings)
    d. Federal Reserve SR Letter 95-51 (Rating the Adequacy of Risk Management Processes and Internal Controls at State Member Banks and Bank Holding Companies) issued November 14, 1995
5 "The Risk Oversight Function of the Board of Directors," Wachtell, Lipton, Rosen and Katz, November 2008.
6 Caremark International Derivative Litigation, reversed Graham v. Allis Manufacturing, holding that the board could not escape liability unless it took some actions to implement a program to detect potential violations of law or corporate policy and exercised a duty of oversight. This is understood to require that the compliance program incorporates procedures by which the board can track and analyze compliance problems that surface and take steps to assure that they do not persist.
7 Stone v. Ritter upheld Caremark International by asserting that the standard in Stone for director liability is whether there is a "sustained or systematic failure of the board to exercise oversight – such as an utter failure to attempt to assure a reasonable information and reporting system exists." This standard aims to protect shareholders by ensuring that corporations will adopt reasonable programs to deter, detect and address violations of law and corporate policy, while absolving the board from liability for corporate conduct so long as it has exercised reasonable responsibility with respect to the adoption and maintenance of a compliance and reporting system. Although the standard protects the board, consistent with most jurisprudence under the business judgment rule, it also requires that the board follow through to address problems of which it has notice; and this may include adopting modifications to its compliance program to address emerging risks. It is significant in this context that good faith on the part of the board will be evaluated within the analysis of whether the board has exercised its duties of care and loyalty, eliminating potential liability where the board has arguably exercised due care, but may not have reasonably considered all of the risks that should be addressed by the compliance efforts, raising the question of good faith.
8 See also Citigroup Inc Shareholder Derivative Litigation, February 2009, Court of Chancery of the State of Delaware and AIG Consolidated Derivative Litigation, February 2009, Court of Chancery of the State of Delaware, February 2009.
9 The Shareholder Bill of Rights, 2009.
10 Public Company Accounting Reform and Investor Protection Act of 2002.
11 Caremark International Derivative Litigation.
12 Ibid.
13 Committee on Oversight and Government Reform – Hearing on the Bankruptcy of Lehman Brothers, October 6, 2008.
14 "An Oversight Oversight," *Risk Magazine*, December 2008.
15 "Enhancing Corporate Governance for Banking Organizations," Bank for International Settlements, February 2006.
16 "The Role of a National Bank Director – The Director's Book," Comptroller of the Currency Administrator of National Banks, March 1997.
17 The top 25 U.S. headquartered banks were selected on their asset size as of March 31, 2009 using a publication from the Federal Reserve's Web site. The five non-U.S. headquartered banks include four European banks and one Asian bank, all of which do business globally. The non-U.S. headquartered banks were selected based on the asset size stated on their respective financial statements. Appendix B "U.S. Headquartered Bank Risk Committees" and Appendix C "Non-U.S. Headquartered Bank Risk Committees" contains a listing of the risk related board committee charters, documenting their committee structure, purpose and duties/responsibilities. Committee charters where based on the board committee charters posted on the organization's Web sites. Where committee charters could not be located, Form 10K or other publicly available governance information related documentation was read to identify board risk committees.
18 "Key Agreed Principles to Strengthen Corporate Governance for U.S. Publicly Traded Companies," National Association of Corporate Directors, March 2009.
19 Ibid.
20 "Putting risk in the comfort zone: Nine principles for building the Risk Intelligent Enterprise," Deloitte, November 2008.

Item #9084