PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP

NEW YORK
1285 Avenue of the Americas
New York, NY 10019-6064
+1 212 373 3000

WASHINGTON, D.C.
2001 K Street NW
Washington, DC 20006-1047
+1 202 223 7300

LONDON
Alder Castle, 10 Noble Street
London EC2V 7JU
United Kingdom
+44 20 7367 1600

TOKYO
Fukoku Seimei Building, 2nd Floor
2-2, Uchisaiwaicho 2-chome
Chiyoda-ku, Tokyo 100-0011
Japan
+81 3 3597 8101

BEIJING
Unit 3601, Fortune Plaza Office Tower A
No. 7 Dong Sanhuan Zhonglu
Chao Yang District, Beijing 100020
People's Republic of China
+86 10 5828 6300

HONG KONG
12th Fl., Hong Kong Club Building
3A Chater Road
Central Hong Kong
+852 2846 0300

June 2009

Board Oversight of Risk Management in Light of Emerging Trends

The fallout from the financial crisis, and the general sense that thinking "outside the box" might have better positioned companies to weather the crisis, are creating greater demands on boards and senior management teams to strengthen risk management practices. Importantly, this trend is no longer confined to banks and other financial institutions. At the same time, recent proposals in Congress intended to address causes of the credit crisis through improvements in corporate governance procedures, and public statements by regulators as to possible future regulatory initiatives, in each case reflecting public sentiment, have focused on risk management structures at U.S. listed companies.

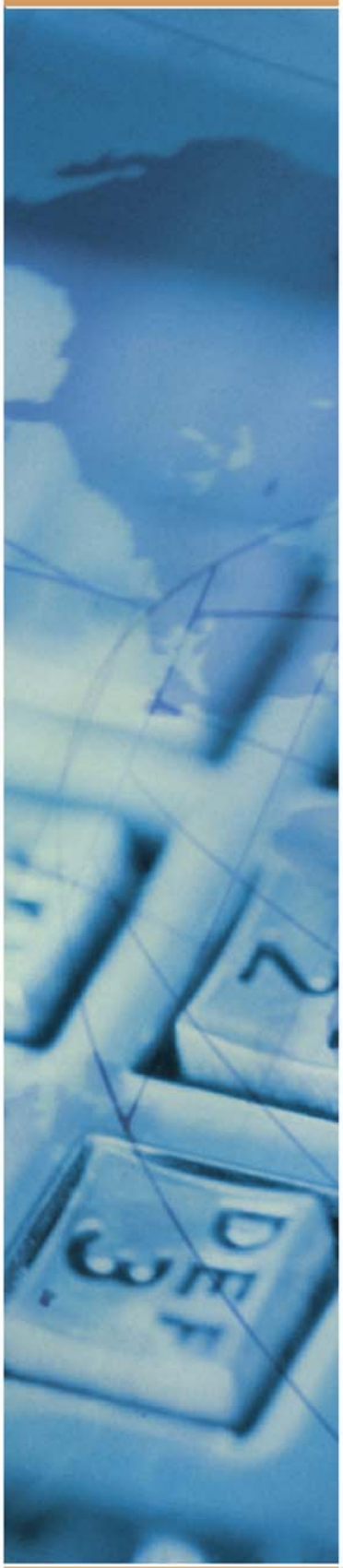
In light of increased demands from shareholders and the potential changes in the regulatory environment, we highlight below a range of considerations for directors as they assess the ways in which they evaluate and oversee risk management processes. First, however, we highlight some of the emerging risk management trends that senior executives are focusing on and provide a brief overview of the regulatory context in which directors are expected to oversee risk management efforts.

Although the discussion below is tailored to U.S. public companies, the considerations could be equally relevant to boards of non-U.S. listed companies, including companies with listings in the United States as well as those that have no direct U.S. nexus.

Emerging Risk Management Practices

Surveys suggest that the financial crisis has led to significant changes in strategic focus and operating models, and it appears that these changes are more frequently occurring in the context of a reassessment of corporate risk profiles. As companies assess their risk profiles, it is becoming increasingly clear that, just as value-at-risk models proved less useful in alerting those charged with monitoring risk to the looming credit crisis and its significant implications, the "one-size-fits-all" approach to risk management is not an answer.

To the extent that approaches are changing, one theme around which risk management programs are coalescing is enterprise risk management ("ERM") – an approach that is by no means a novel idea (see, for example, the 2004 Integrated Framework developed by the Committee on Sponsoring Organizations of the Treadway Commission), but is gaining more adherents as companies outside the financial services sector turn their attention beyond internal controls to more broad-based risk management assessments. ERM is intended to avoid the



"silo" mentality whereby risks are addressed by the relevant functional area only, without triggering a broader assessment of how particular risks might affect an enterprise as a whole.

Companies embracing ERM's more "holistic" approach to risk management may focus on a broad set of initiatives that have the following core elements: Senior management should, on a regular and periodic basis, undertake risk assessments aimed at identifying the full range of key risks that an enterprise may face, the probability of occurrence of those risks and the potential impact of the more material among them on the enterprise's business and prospects. A key element of the assessment will be a recognition that risks can originate from diverse, and unexpected, sources. The assessments should be combined with an evaluation of the ability of risk management processes to provide an early warning of the potential range of risks. The focus is likely to be on the wider impact of the risk to the enterprise as a whole, rather than merely its impact on financial performance. As part of this effort, senior management will likely introduce sensitivity analyses and scenario planning for the more prominent risks.

Although no single list will be complete, it is fair to assume that management teams will focus on many of the following key areas regardless of which industry sector they operate in:

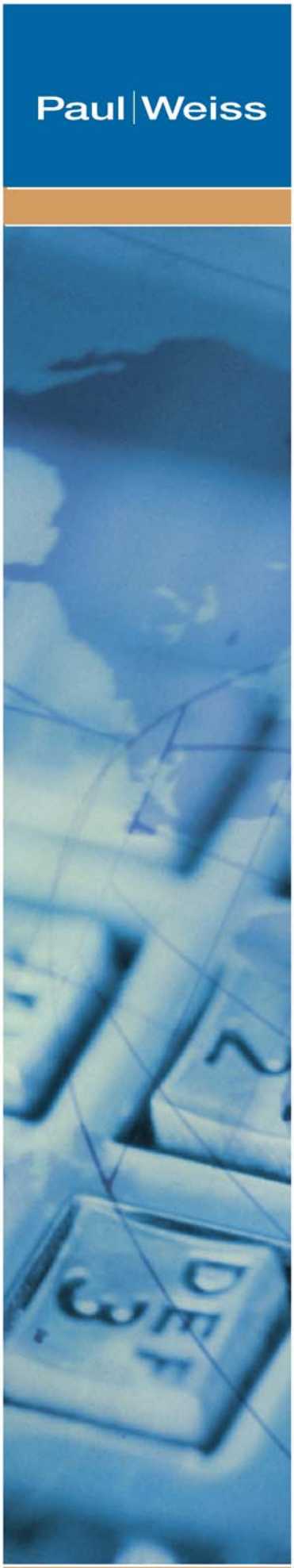
- vulnerabilities to the current credit environment;
- exposure to current global economic conditions;
- viability of the company's current strategic focus and business plan;
- the potential impact of regulatory changes;
- the ability to implement cost saving measures and the implications of rolling out those measures;
- counterparty risks;
- changes in the competitive landscape;
- emerging issues, such as climate change, which can have consequences ranging from changes to business models to potential litigation exposure;
- retention and compensation of senior executives and other key employees; and
- reputational risk.

Regulatory Trends in Risk Management

Risk management, in its broadest sense, in the non-financial sector is a relatively recent topic. Directors are generally aware of their fiduciary duties (as developed under applicable state law) and their role in a range of oversight functions (many focused on internal control and the integrity of the financial reporting process) that were enhanced significantly as a result of the Sarbanes-Oxley Act. However, there has been little guidance as to the nature of the obligations in respect of risk management that arise under general notions of duties owed by directors.

Existing Guidance

In Delaware, courts have held that directors' obligations include a duty to "attempt in good faith to assure that a corporate information and reporting system, which the board concludes is adequate, exists." See *In re Caremark International Inc. Derivative Litigation*. In *Caremark*, the court held that directors are liable for breach of fiduciary duty only in the event of 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." Since then, subsequent cases have confirmed that standard and also noted that liability can arise where, having implemented such a system, directors "consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention." See *Stone v. Ritter*, and *In re Citigroup Inc. Shareholder Derivative Litigation*. The court in *Stone v. Ritter* approved the *Caremark* standard and clarified that liability would be based on the concept of good faith, which is embedded in the duty of loyalty and does not constitute a separate fiduciary duty.

The corporate governance listing standards of the New York Stock Exchange include among the duties of an audit committee the responsibility to discuss policies with respect to risk assessment and risk management. The commentary to that provision states that,

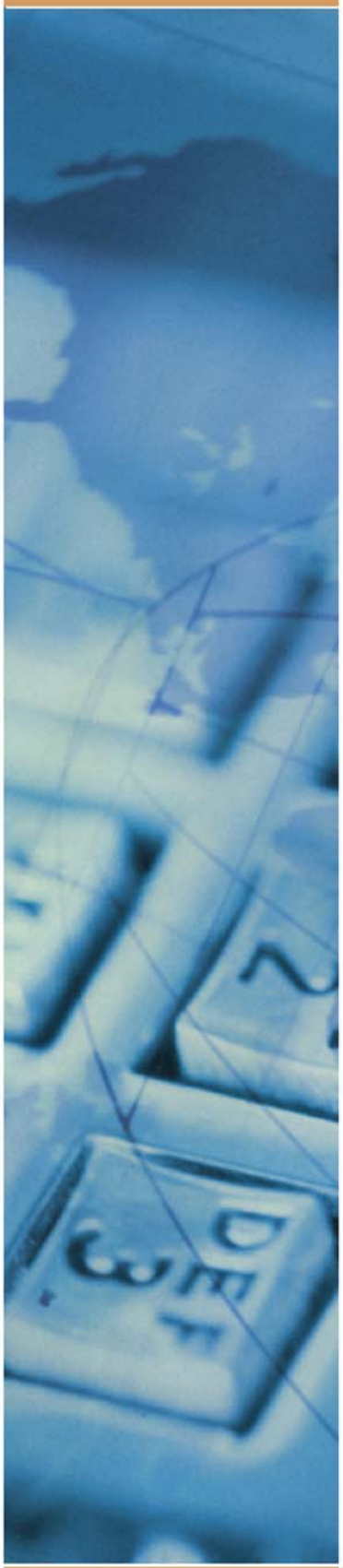
> "[w]hile it is the job of the [chief executive officer] and senior management to assess and manage the listed company's exposure, the audit committee must discuss guidelines and policies to govern the process by which this is handled. The audit committee should discuss the listed company's major financial risk exposures and the steps management has taken to monitor and control such exposures. The audit committee is not required to be the sole body responsible for risk assessment and management, but, as stated above, the committee must discuss guidelines and policies to govern the process by which risk assessment and management is undertaken. Many companies, particularly financial companies, manage and assess their risk through mechanisms other than the audit committee. The processes these companies have in place should be reviewed in a general manner by the audit committee, but they need not be replaced by the audit committee."

SEC rules applicable to reporting companies tend to focus on disclosure and few of the applicable requirements are tied directly to risk management. The risk management provisions of the Emergency Economic Stabilization Act of 2008 apply only to companies participating in the Capital Purchase Program and are geared towards ensuring that incentive compensation for senior executives does not encourage "unnecessary and excessive risks that threaten the value of the financial institution."

Emerging Themes

In recent weeks, attention has turned to corporate governance reforms and enhanced disclosure as means to improve risk management oversight. The proposed Shareholder Bill of Rights Act of 2009 would require listed companies to establish an independent risk committee responsible for establishing and evaluating risk management practices.

Separately, the Chairman of the SEC has stated that the SEC will be considering several proposals requiring greater disclosure of items that bear on risk management. The SEC is considering, for example, whether to enhance disclosure requirements concerning director nominee experience, qualifications and skills in order to augment current requirements that are limited to a brief description of a candidate's business experience over the past five years. The SEC is also considering whether to require disclosure of the reasons why a board has chosen a particular leadership structure; whether to require greater disclosure of how a company, and particularly its board, manages risks, generally and with respect to setting compensation; and whether greater disclosure is needed regarding a company's overall compensation approach (beyond its highest paid officers), as well as compensation consultant conflicts of interests.



If U.S. listed companies are required to establish risk committees, boards will need to consider various issues: the role of any such committee in light of their company's risk profile, the nature of the interface between the risk committee and other board committees; and how best to discharge the ultimate responsibility of the full board. Composition of the risk committee will also need to be considered, particularly if the independence standards follow current audit committee requirements and if directors are expected to provide more disclosure regarding skills and experience. Note that, particularly as a result of the corporate governance changes that followed the passage of the Sarbanes-Oxley Act, audit committee members often are chosen for experience and skills tied to financial reporting, and that risk management is far broader than internal control, disclosure controls and other procedures that evolved in response to the financial scandals of the 2001-2003 period.

Areas of Focus

Whether it is in response to potential changes in corporate governance rules, or more likely because it is the right thing to do, a board should focus on ensuring that the company has in place effective risk management processes tailored to the types of risks the company is likely to face. The board should focus on whether the risk management processes established by management are in fact tailored to the company's risk profile and on whether the company's appetite for risk corresponds to its strategy and objectives. The board should also ensure that it has struck a reasonable balance between full board responsibility, on the one hand, and committee (delegated) responsibility for risk management-related tasks, on the other.

As part of its oversight function, the board should:

- assess the quality of the information it is receiving;
- assess how well it understands the company's business and the risks the company faces;
- assess how management evaluates risks;
- assess the quality of the risk management oversight structure; and
- consider lessons learned.

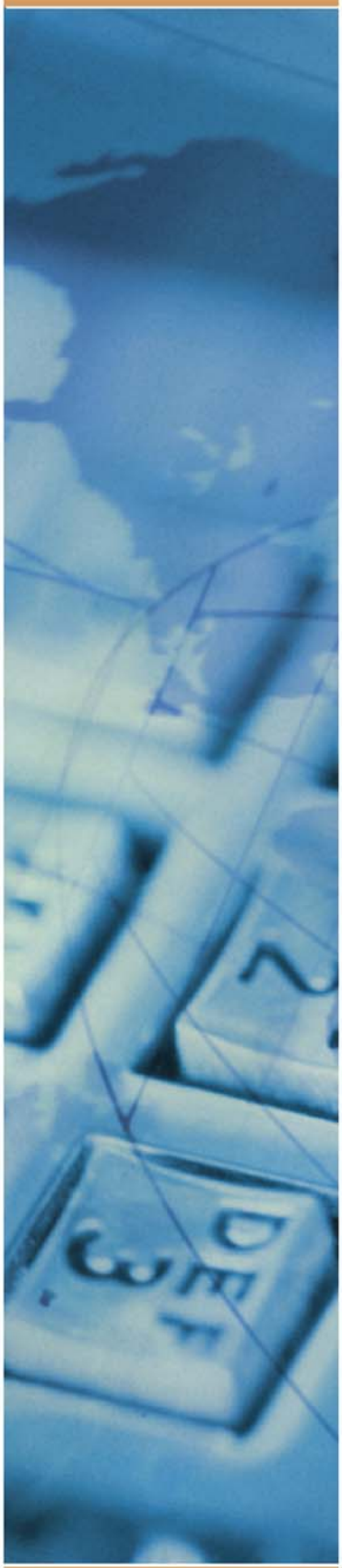
We address each of these below.

Assess the quality of information

Directors are generally dependent upon management for information about the company, its performance and its prospects. Management typically controls the information flow through the setting of meeting agendas and the selection of information that is presented at board and committee meetings. The critical question then is whether the directors are comfortable with the scope, relevance, timeliness and clarity of the information they are receiving.

Many boards, and audit committees in particular, have responded to the current financial crisis by enhancing their level of interaction with management teams. This may take the form of regular update calls with the chief financial officer, the chief accounting officer and/or the treasurer, invitations to a broader group of executives to attend board and committee meetings, lengthier executive sessions, including sessions at which the chief executive officer may appear by himself/herself, and more frequent and more in-depth questions addressed to senior management. Boards and committees are typically meeting more frequently, and are covering a

Paul|Weiss



broader range of items and in greater depth. Risks and the effective management of risks are becoming a more frequent agenda item.

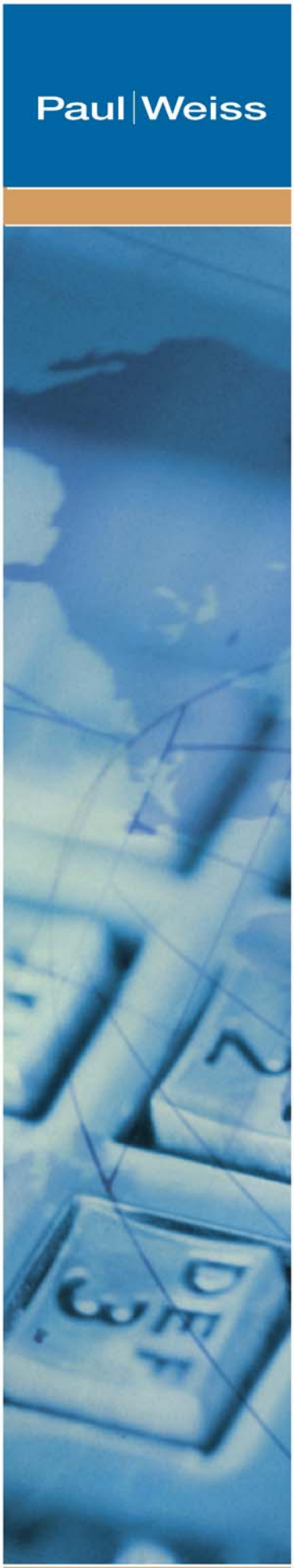
As directors consider the information they receive, they should:

- Consider whether management is facilitating the free flow of information and effective interaction.
- Consider whether the key performance indicators, key assumptions underlying potential risk, and information as to the likelihood and magnitude of potential risk are appropriate to the company's risk profile.
- Ask management to describe how it assesses and prioritizes potential risks and how frequently it makes these assessments. What assumptions are used and what are the implications of changing the underlying assumptions? How have conclusions changed over time?
- Obtain input from auditors, counsel and consultants to test the conclusions reached by management.
- Consider seeking risk assessments conducted by principal customers or suppliers about the company.
- Reach out to a broader group of executives within the company. Consider speaking with heads of business units and foreign-based executives. Remember that, in some cases, the source of significant risks to an enterprise has been a smaller operation that does not figure prominently on the risk radar screen.

Understand the business and its risks

Having more information is not an end in itself. Rather, it is important that the information can be put into context, understood and, when needed, acted upon. Above all, directors should understand the relationship between risks, on the one hand, and the company's strategy and business plan, on the other. As part of that process, directors should:

- Engage in open discussions with management on how the financial crisis affects or may affect the company's strategic goals, operations and performance. Evaluate how different management assumptions affect strategy, forecasts and the risk profile of the company. Remember that as strategy is re-assessed and revised, the company may face different risks.
- Review the company's periodic and current reports and prospectuses, with a particular focus on risk disclosures. In particular, directors should ask the following questions about such disclosures:
    - Do the disclosures reflect the risks that the board and management have identified and discussed, and concluded are relevant?
    - Are the disclosures comprehensive enough and at the same time easy to understand?
    - Are the procedures that support the chief executive officer/chief financial officer certification process appropriate?
    - Is it advisable to abstain from providing earnings guidance?



  - What did the disclosure committee decide not to disclose in the company's periodic and current reports and other filings?
- Review periodic and current reports and prospectuses of competitors, as well as analyst reports covering the company and the industry.
- Review the results of stress tests or other sensitivity analyses that management conducts.
- Review hedging strategies.
- Request management to provide a broad assessment of counterparty risk.

Encourage a "holistic" view of risk management

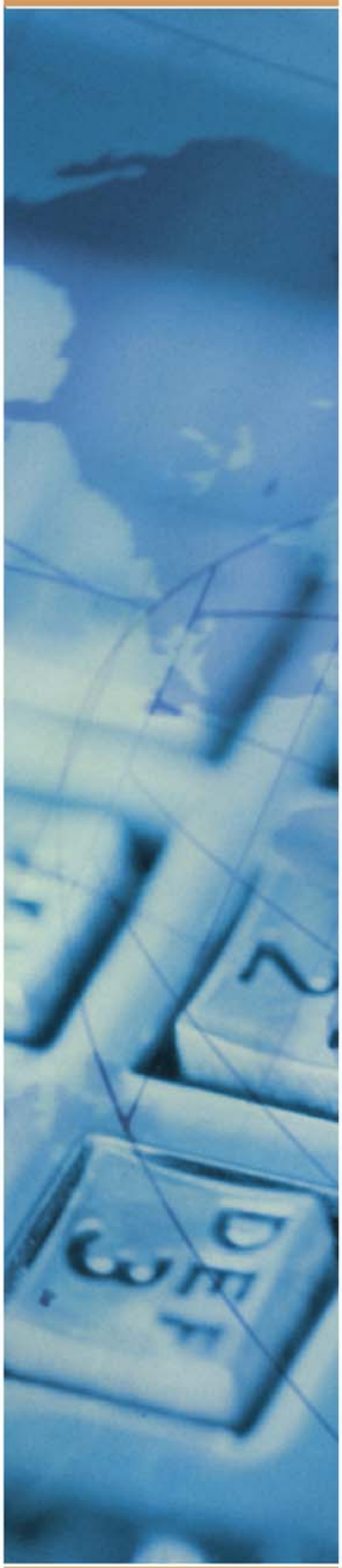
With a better understanding of the ways in which the company is exposed to risk, the directors will be in a better position to then focus on the process by which those risks can be anticipated and managed. At this point, directors should:

- Ensure that management is focusing on the full range of potential risks: operational, financial, capital, liquidity, market, counterparty, regulatory and reputational.
- Ensure that management focuses on where and how risks originate and how well the company is positioned to deal with the risks. These could include, for example, regulatory changes, the impact of emerging litigation trends (such as in respect of climate change), liquidity constraints faced by counterparties or the impact of internal cost cutting measures.
- Ensure that management considers the correlation between different types of risk in its decision-making.
- Test management on how risks have shifted, or are shifting, over time.
- Understand the qualitative and quantitative criteria used by management for rating risks on the basis of impact and likelihood of occurrence.
- Assess the risk-tolerance thresholds used by management to determine when risks need to be escalated to the board (or a designated committee).
- Challenge the assumptions upon which management's conclusions are based. Suggest that management apply different assumptions and scenarios in risk models.
- Ensure that management considers the impact of operational and structural changes on the risk management process itself.
- Ensure that management develops a crisis response plan that is sufficiently comprehensive.

Evaluate organizational structures and processes

Ensuring that the organizational structure of the company is geared towards effective risk management is an integral part of the oversight process. In that connection, directors should:

- Consider the need for a chief risk officer. If one is appointed, ensure that the chief risk officer reports directly to both the chief executive officer and the board.
- Review and evaluate the role of internal audit and the chief risk officer in the risk management process, and recognize that each performs different functions.



- Subject to possible new requirements, consider the need for a separate risk committee and, if one is established, consider the respective roles of the audit committee and the risk committee. Consider joint meetings from time to time to ensure comprehensive coverage, without unnecessary duplication.
- If the risk management function is supervised by the audit committee, provide for periodic reviews of risk management processes by the audit committee, separate from its role in the oversight of financial reporting.
- Consider how best to enlist the general counsel in assessing potential risks to the company. Is the role of the general counsel broad enough to encompass evaluation of the risk landscape from a legal and regulatory standpoint, and is the general counsel tasked with reporting on trends as well as historical concerns?
- Is the disclosure committee staffed with the appropriate people?
- Evaluate "management risk" – the risk that management is not ideally suited in the current environment to manage the risks that the company may face.

Consider lessons learned and remain engaged

As noted at the outset, no single approach will work for every enterprise. We offer two final themes to consider. First, it is useful to keep in mind the types of deficiencies that conventional wisdom now associates with the crisis, and to consider whether any of these currently apply to the enterprise in question:

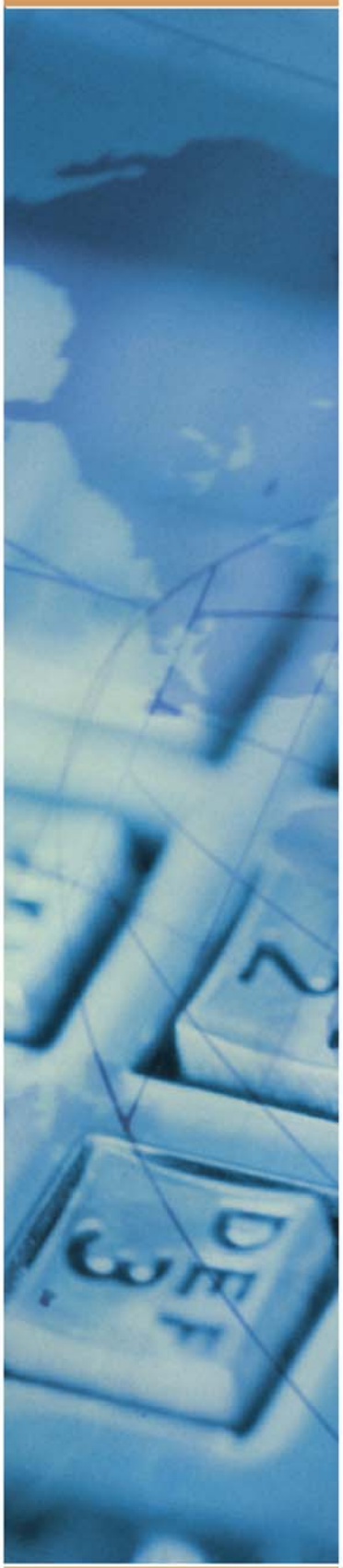
- risk managers underestimated correlations of risk;
- risk managers relied too heavily on historical data in developing risk models;
- risk management was approached based on functional area (the "silo" mentality) and failed to take an enterprise-wide view of risks;
- management focused on fraud, financial reporting irregularities, theft, IT-related risks and the like to the exclusion of other risks;
- management failed to appreciate the link between strategy and risk;
- overall responsibility for risk management was ill-defined; and
- processes for reporting "red flags" were inadequate or when reported "red flags" were ignored.

Second, remember that the full board needs to remain engaged with, and aware of (through regular reports and discussions), risk management issues. Creation of a separate risk committee, or delegation of risk management oversight functions to the audit committee, will not relieve the directors generally of their oversight responsibilities. Note too that each of the other board committees will have their own risk management perspectives (whether management succession for the nominating committee or executive compensation for the compensation committee). Reliance on committees should not itself create a "silo" approach at the board level that fails to address the full range of risks that an enterprise may face.

* * * *

In the coming weeks and months we are likely to see the details of various proposals relating to risk management and evaluation and disclosure of risks. Any proposal mandating the

Paul|Weiss



establishment of risk committees is likely to be subject to intense debate, and should such committees be required for all U.S. public companies, one likely question will be who will serve on such committees. Composition of such committees will be of particular interest given the fact that calls to require formation of such committees have been motivated in part by concerns that audit committee members currently have a significant workload.

At this point, boards and senior management teams need to be aware of these trends and to position themselves and their companies to remain ahead of emerging issues. These issues should be addressed without creating an environment in which reasonable levels of risk, which are, and should continue to be, proper elements of strategy and operations, are avoided in the name of risk management.

* * * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content.