THOMSON REUTERS ACCELUS™
BUSINESS LAW CURRENTS

ACHIEVING MORE EFFECTIVE RISK OVERSIGHT IN AN UNCERTAIN ENVIRONMENT

OCTOBER 6, 2011

MARK S. BERGMAN, PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP

(Thomson Reuters Accelus) The growing level of uncertainty in the global marketplace and increasing complexity in many sectors -- due to factors ranging from volatile currency markets and continued constraints on credit to greater regulatory activism -- underscore the importance of risk oversight at the board level and risk management at the management level.

In the past three years, the financial crisis clearly has led to soul-searching in boardrooms, as well as among regulators and politicians, as to what could have been done to better anticipate the events that led to unprecedented turmoil in the financial and credit markets. These efforts invariably focused on risk management.

Since the crisis, various other factors have served as catalysts for boards and management teams the world over to focus on risk. These factors have included corporate governance reforms adopted in various jurisdictions following the crisis, new disclosure obligations in respect of corporate governance, shareholder activism, changes in rating-agency criteria, greater enforcement of anti-bribery and trade sanction rules, and emerging risks such as cyber-crime and climate change, among others.

While the principal "first movers" in restructuring risk management and risk oversight processes were financial service companies, enterprises in non-financial sectors have also embraced the new focus on risk. If post-financial crisis examples were needed for those outside the financial sector to understand the benefits of comprehensive risk processes, disruptions of the supply chain following the earthquake and tsunami in Japan served as stark reminders of the need to think about, and plan for, the unthinkable.

Uneven Progress to Date

From the perspective of directors as well as management, progress in the area of risk oversight has been uneven. There may be agreement that some level of risk is good and, in fact, is necessary for growth. While management is more likely to view risk management as presenting opportunities, there remain tensions between the view that risk management is about shaping the future direction of an enterprise to capitalize on growth opportunities and the view that risk management is all about protecting the franchise. In fact, it is a combination of the two – and finding the right balance is the key.

Obviously, the level of progress in enhancing risk management and risk oversight functions, and the perceptions among directors and management teams regarding the efficacy of such functions, invariably will differ not only as between financial services firms and non-financial service firms, but also between listed companies and private companies, and between large companies and smaller companies. Nonetheless, some general themes have appeared.

- There is not enough clarity around the concepts of **risk oversight** and **risk management** and as to the proper roles of directors in the risk framework.
- While much emphasis has been placed on policies and procedures, this emphasis may be somewhat counter-productive, with significant time being spent on controls and monitoring, and less time being available to understand the **risk culture** and understand whether the proper risk culture has evolved.
- Corporate governance reform may exacerbate the focus on process and compliance at the expense of implementing and monitoring effective **risk controls**.
- Not enough has been done to focus on **emerging trends** such as climate change and sustainability; risk horizons tend to be short.
- Risk management tends to be too focused on the enterprise itself and not focused sufficiently on **external metrics**.
- While an increasing number of companies are hiring Chief Risk Officers (CROs), there are concerns that CROs do not have the proper mandate to play a greater role in **strategic decisions**.
- Not enough time is spent at the board level understanding the relationship between **risk appetite and strategy** and in evaluating the potential risks associated with initiatives to implement corporate strategy.
- Directors have difficulty absorbing all of the **risk-related data** they are given.
- Directors would like more comprehensive risk reporting to the board, particular in respect of **emerging risks**.
- Boards should have greater access to **external sources of data** on risks.
- More should be done around **stress testing**.

Defining the Risk Oversight Function

For directors seeking to better understand their role, the key is to understand the difference between risk oversight and risk management.

Although there is no uniform definition of risk oversight, there are common elements. The function certainly involves understanding the key risks the company faces and may face in the future. The function should involve an ongoing dialogue with management regarding risk appetite and whether strategy is consistent with risk appetite. Finally, the function requires an understanding of management's risk management procedures and monitoring of the effectiveness of risk management procedures.

Risk management, on the other hand, describes the initiatives of management to: (a) identify, quantify, monitor and report, and mitigate the key risks to the business, its corporate strategy and the implementation of that strategy, (b) help establish, and then communicate to the organization, the risk appetite, and (c) establish the proper risk culture. Central to this endeavor will be the parameters set around risk appetite and risk tolerance.

Board Action Items

Effective risk oversight should not be viewed as a check-the-box exercise or a static undertaking. With ever-changing risk landscapes, risk management structures should be tested regularly to ensure they are evolving as risks and risk oversight needs evolve to take account of the dynamic nature of the challenges management teams will face. For directors wishing to better understand their risk oversight role, I have set forth below a list of action items.

1. Determine the appropriate board-level structures to address risk oversight – full board, audit committee or risk committee.
   - Note different business require different approaches
   - While risk oversight is a board responsibility, certain functions can be delegated to one or more committees
   - Is enough time allocated to risk oversight matters, particularly when this includes discussions of strategy and risk appetite
2. Evaluate the skill set at the board level; consider benefits of board turnover; consider the benefits of board diversity; and consider the ability to have candid discussions and to ask the tough questions.
   - There is no universal agreement on the right skill set
3. Consider the benefits of a CRO and the proper mandate.
   - The CRO can provide input on strategy
   - The CRO should in any event facilitate aggregation of risk data
   - The CRO should have the requisite mix of experience and skills
4. Understand the broad universe of risks and the most significant risks and that risks can be strategic or operational. Although there are different ways of categorizing risks, they are likely to include:
   - Competition
   - Customer
   - Supply chain
   - Market
   - Credit
   - Counterparty
   - Financial
   - Regulatory and compliance
   - Information technology (including security of customer and proprietary data)
   - Human resources
   - Health and safety
5. Understand the difference between risk management and risk oversight; articulate an approach to risk oversight that is appropriate for the company and its business – based on acceptable risk appetite, complexity of the risks the business faces and the regulatory environment.
6. Evaluate the company's risk appetite and its relationship to strategy; communicate the board's view of the company's risk appetite and ensure that the message is communicated throughout the company.
   - All enterprises have a risk appetite; they may not characterize it as such
   - Recognize that not all risks are measurable
   - Evaluate the risks that are acceptable and the ones that are not, and set the risk tolerances on that basis; agree on acceptable frameworks for evaluating the enterprise's risk appetite and the appropriate limits. For example:
     - what limits are imposed in connection with the launch of new products, penetration of new markets or conducting business in new countries
     - what are acceptable levels of debt
     - what parameters are in place in respect of hedging arrangements
     - what is deemed to be an acceptable negative impact on earnings

- what are appropriate target financial ratios or target credit ratings
- what are the minimum conditions for organic growth versus growth by acquisition, or joint ventures
- what are acceptable headcount levels given the enterprise's existing infrastructure, and what levels would be required as the enterprise grows
- what are acceptable sources of financing
- what are appropriate levels of R&D
- what are the implications of customer concentration
- what are the implications of competition
- what limits are applied to insurance arrangements, including captive insurance programs; how might risk transfer and capital management coverage benefit the company

7. Understand management's risk management processes and how those processes are applied across the enterprise. Remember that significant risks to the enterprise may arise in smaller business units or in other unexpected (or remote) areas of the business.
   - Pose the "what if" questions and challenge existing assumptions
   - How are deviations from risk limits handled
8. Periodically evaluate whether developments in the risk landscape have been factored into risk management assessments and strategic decisions.
   - Changes in market conditions, the mix of business, the competitive landscape, the legal or regulatory landscape, macro economic conditions and the geopolitical situation, to name a few, can have an impact on risk considerations, and hence on strategy and business plans
9. Assess the way in which the board seeks to perform its risk oversight function; consider the timing and content of management reporting to the board on risk; ensure there is agreement with management on what should be elevated to the board, when and in what form; and be aware that potentially significant risks may not at first be obvious
   - Is the board fully satisfied with the monitoring and reporting of risks to the board
   - Is sufficient time allocated to risk oversight matters
   - How frequently are the most significant risks reported to the board
   - How frequently are management's processes and procedures reviewed
   - How frequently are emerging risks and the changing landscape discussed with the board
   - To what extent are risks measured on an aggregated basis
   - How frequently are gap analyses performed and reported to the board
   - How frequently are "remote" risks and worst-case scenarios analyzed and reported to the board
   - Does the board assess the level of resources devoted to risk management
   - If risk limits are exceeded when are these circumstances reported to the board
   - Has the board addressed crisis management procedures
10. Obtain external perspectives, particularly in respect of global operations and emerging risk areas. These could include:
    - Presentations by auditors, outside counsel, risk consultants or business intelligence firms
    - Research reports covering the company, its competitors and the industry
    - Summaries of the public disclosure of competitors
11. Reach out to others in the company beyond the CEO, CFO and CRO to get a sense of the risk culture and test risk assumptions.
    - Input is likely needed from heads of business units, the chief legal officer, auditors, and the heads of information technology, human resources and investor relations
    - Information passed up through the ranks may be distilled to such an extent that important considerations may be lost
    - What are the escalation processes for reporting risks to senior management and the board
12. Recognize the overriding importance of "tone at the top."
    - Risk considerations should be integral to business planning, including expansion of the business into new products, new markets and new countries and expansion through acquisitions or joint ventures
    - Responsibility for risk management should be clearly defined and consistently applied across the enterprise
    - Sufficient resources (with the requisite experience and skills, and the requisite authority) should be allocated to risk management
    - Management should be proactive in involving the board
    - Management needs to communicate that it fully embraces risk management and appreciates the importance of risk management processes
    - There should be a culture of open dialogue and candor; red flags should not be ignored; potential issues should be timely escalated to the proper levels

- Adherence to risk limits and risk tolerances should be factored into compensation and promotion decisions; failure to adhere must be properly addressed
- Management should follow up on identified gaps
- Internal compliance programs (to address fraud, bribery, regulatory compliance, and the like) and whistleblower programs (subject to local legal requirements) should be carefully written and evaluated on a periodic basis; directors, senior management and other employees should receive the appropriate level of training and have access to relevant, clear and concise compliance guidelines

13. Consider whether the company has succession plans in place, particularly to address unexpected departures of senior executives.

14. Ensure that the enterprise has contingency plans, with well defined crisis management protocols and communications strategies.

15. Evaluate the board's risk oversight efforts.

Communicate, Review and Update

As concerns over sovereign debt and rates of economic recovery continue to mount, and in an era when business has become more global and more complex, laws and regulations often are becoming more restrictive and bad news can go viral in an instant, risk oversight and risk management must be uppermost in the minds of corporate directors and management.

At a minimum, directors need to remain mindful of the following key elements: strategy and risk appetite must be assessed together, responsibilities need to be clearly delineated as between the board and management, expectations must be properly communicated throughout the organization, adequate and appropriate resources need to be mobilized at the board and management levels, and systems and contingencies need to be regularly reviewed and updated.

The views expressed in this contributed piece are the author's own.

ABOUT THE AUTHOR

Mark S. Bergman is a partner at Paul, Weiss, Rifkind, Wharton & Garrison LLP, a resident in London and co-head of the firm's Global Capital Markets and Securities Group.