The Bulletin

protiviti®

VOLUME 3 ISSUE 6

Ten Common Risk Management Failures and How to Avoid Them

It is fashionable today to talk about the role of risk management in the global financial crisis. Indeed, risk management had a role – a very important one. As we look back and closely examine what has transpired, we often hear the same questions expressed with a noticeable point of inflection in the voice pitch: What were they thinking? What did they know? How did they let this happen? Because the crisis has had such ominous consequences for the global economy and our very way of life, we thought it appropriate to step back and reflect on why risk management fails in any industry. Accordingly, this issue of *The Bulletin* explores 10 common risk management mistakes and how they can be avoided. It is based on our firm's collective experiences in working with many companies, as well as seeking to understand significant failures observed over the years.

Failure No. 1: Poor Governance and "Tone at the Top"

Effective governance and tone at the top drive the transparency, openness and commitment to continuous improvement that is needed for risk management to function effectively. A leadership failure will almost always undermine even the strongest risk management capabilities.

Following are some key indicators that this issue exists within an organization:

- A dominant chief executive ignores the warning signs posted by risk management and resists bad news or facts suggesting his or her strategy is not working.
- Management does not understand the nature of the risks undertaken by the organization.
- Risk is not considered explicitly by management when evaluating whether to enter new markets, introduce new products or consummate a complex acquisition or investment.
- Management does not involve the board with strategic issues and policy matters in a timely manner.
- There is ineffective or nonexistent communication of risk information up, down and across the organization.

We believe that governance is the establishment and maintenance of a flexible corporate structure that balances the enterprise's objectives and performance goals to *create* enterprise value with the policies, processes and controls it deems appropriate to *protect* enterprise value. Too often, the focus is on the short term – the next month, quarter, etc. – which causes organizations to take risks by mortgaging the future for the present. We see this near-term focus across the board in many corporations today. While balancing value creation and protection, as well as the present and the future, is a relatively straightforward concept, pulling it off requires effective leadership and discipline.

The board and management can do several things to ensure that governance and leadership place importance on the contributions of risk management and drive a culture of "sustainable value." First, the board, with management's assistance, can conduct a governance assessment to understand how risk management and compliance management are set up to function within the organization and ensure that the policy structure, accountabilities, direct lines of reporting and escalation protocols are all conducive to effective governance and the flow of communications. Second, directors should watch for the existence or emergence of warning signs such as undeliverable strategies, extreme performance pressures, unrealistic expansion plans, inadequate executive experience, a myopic short-term focus, incentives for excessive risk taking, evidence of a "warrior culture" and unhealthy internal competition, and signs within the ranks that there is a "fear of the boss." A combination of these warning signs points to a lack of leadership that can compromise risk management. Finally, the board should exercise strong oversight when management desires to enter into a line of business that it has no experience in managing and, therefore, may not understand the related risks. This oversight should include explicit discussions with executive management regarding the enterprise's appetite for risk.

Failure No. 2: Reckless Risk Taking

A lesson we keep learning is the need for more disciplined risk taking during periods of rapid growth and favorable markets. Every MBA program features case studies of companies relearning the time-honored lesson that, although competent people are an important aspect of managing risk, management's reliance on them without limits, checks and balances, and without independent monitoring and reporting is as ill-advised as not understanding the risks inherent in what they are doing. It is interesting that companies, even entire industries, keep relearning this fundamental lesson. Indeed, in the current financial crisis, there is evidence that astute students of past crises fared better this time around.

Some key indicators of this problem include:

- Responsibility for risk management is not adequately defined or linked to the reward system or, worse, the incentive compensation program rewards unbridled risk taking.
- There are "star performers" who are making a great deal of money but no one understands how.
- There are large, unknown risk exposures representing "ticking time bombs" – and management is not aware of them.
- The board is not providing sufficient oversight.
- There are significant conflicts of interest in complex, volatile and/or difficult-to-measure areas.

How to avoid this costly failure? Following are points to consider:

- First, understand how you are making money and the risks inherent in your business model. Often, achieving this understanding means applying the familiar 80-20 rule; that is, a majority of a firm's success often comes from a much smaller segment of its activities. What are those activities? Who executes them? Who oversees them? How and why do they make money? What are the risks inherent in them? Push back on the "smartest people in the room" and avoid presuming they know what they are doing because they are making money.
- Second, identify and manage your trust positions, meaning the people whose actions or inaction can subject the enterprise to significant risk events. Who are these people? Where are they, and what are they doing? Who oversees them? These positions are not limited to financial-related risks.
- Third, pay attention to how your organization's incentive compensation structure and culture drives behavior. Are there potential unintended consequences that management and the board would want to avoid?
- Finally, establish accountability for results and create a process for timely escalation. Transparency is an important objective and should be emphasized to facilitate discussions about prudent risk-taking, risk-based communications, effective enterprise risk assessments that impact business planning, and periodic scenario analyses to evaluate assumptions underlying the strategy, among other things.

Failure No. 3: Inability to Implement Enterprise Risk Management (ERM)

This failure is one we see time and again. Most efforts to implement ERM are unfocused, severely resource-constrained and pushed down so far into the organization that it is difficult to establish their relevance. The near-term result is "starts and stops" and ceaseless discussions focused on understanding what the objective is. The longer-term result is that risk management is never elevated to a strategic level and is driven by functional silos within the organization.

Common indicators include:

- Lack of executive management support and involvement of the right people
- Lack of clarity as to the business motivation, leading to endless dialogue about the "what" and "why"
- Lack of traction due to delegation of initiative to lower levels in the organization
- Viewing the existing risk management silo functions as "ERM" since they cover the risks
- An ERM initiative that is neither enterprisewide in scope nor strategic in focus
- Noncompliance with the organization's risk management policy

The board and management should empower a group of senior executives to define the role of risk management within the enterprise. This perspective should be supplemented with an enterprise risk assessment and capability gap analysis to answer two questions: What are our priority risks, and how well are we managing them? The results should be used to prepare a compelling business case and economic justification for elevating risk management to a strategic level within the enterprise. Management should look for quick wins by focusing on the areas in obvious need of improvement. Throughout the process, the board of directors should be involved.

Failure No. 4: Nonexistent, Ineffective or Inefficient Risk Assessment

This failure arises when risk assessment activities are not identifying key risks effectively, efficiently and promptly. We often see a relevancy issue when management experiences difficulty in translating issues identified by a risk assessment into actionable steps that can be included in a business plan. As a result, the enterprise practices ELM (Enterprise List Management) instead of ERM because nothing happens when a risk assessment is completed beyond sharing the most current list of risks among company executives.

Some key indicators are:

- Multiple risk assessments besiege the entity's process and functional owners due to a silo mentality.
- Risk management silos and the lack of a process view allow significant risk issues to go unnoticed.
- General counsel inhibits the risk assessment process with concerns over risk documentation.
- Periodic risk assessments rarely impact business plans and decisions.

To improve the effectiveness of the company's risk assessment activities, management should first develop a common risk language and implement a rigorous and consistent enterprisewide risk assessment process. The process should involve key stakeholders and focus on what is really important – the vital strategic risks – as opposed to minutiae. It is important for the risk assessment to be linked to the business plan. Finally, management's evaluation of results should be reported to the board of directors to obtain their input and perspective.

Failure No. 5: Falling Prey to a "Herd Mentality"

While ineffective risk management certainly contributed to the financial crisis, there were other causal factors, such as lax regulation, awry financial innovation, nonexistent underwriting standards, over-the-top debt, and the motivations driven by the short-term focus of incentive compensation programs. The tipping point was the sheer volume of activity by mortgage brokers, lenders, mortgage insurers, investment banks, credit default issuers and institutional investors. Not enough of these players knew when to stop. It is one thing to engage in legitimate business activity. It is quite another to know when the risks of doing so have reached an unacceptable level. Too much of a good thing can become a bad thing when following the herd.

Some key indicators of this problem are:

- Management continues to execute the same strategy and business model, regardless of whether market conditions suggest the assumptions underlying the strategy may be invalid.
- Management approaches the planning and budgeting process with a single-point estimate or view of the future.
- Alternative scenarios are rarely considered in periodic stress tests of financial models.
- The organization is too insular in its outlook, leading it to not "reality test" its assumptions about markets and the operating environment regularly.

To avoid this failure, management should:

- Undertake a detailed review of the organization's financial condition.
- Re-examine and challenge business and operating models in light of changes in the operating environment.
- In lieu of a singular view of the future, consider multiple views of the operating environment over the planning horizon to assess how the strategy would perform.
- Introduce more extreme scenarios into stress tests of financial models, including credit and market risk exposures.
- Ensure the strategy-setting process allows for periodically evaluating how well the strategy is performing.

Failure No. 6: Misunderstanding the "If You Can't Measure It, You Can't Manage It!" Mindset

A prevalent view is that if you can't measure a risk, you can't manage it. While this mindset is largely true, many managers often use it as an excuse to do nothing at all with respect to understanding and addressing a difficult-to-measure risk. Because inability to measure a risk will not make it go away, managing solely to the measurable is never enough and ignores important issues that ought to be on the screen of decision-makers.

Key indicators include:

- Confusing qualitative risk maps with "risk measurement"
- Existence of large risk exposures for which there is little data and information
- Lack of a continuous-improvement mindset in risk management and, in particular, risk measurement
- Management believes that risk measurement and risk management are the same thing
- Confusing "data" with "information"

The latter two points bear further mention. We believe that financial services firms became too focused on what their models said and did not exercise enough judgment. We also believe that many firms received reams of data but very little of it was useful from a decision-making standpoint in dealing with the developing concentration, basis and correlation risks.

To avoid this failure, management should:

- Identify the priority risks and determine the extent of relevant data and information available for each risk.
- Determine additional information needed to better understand the risks and the available sources to use for purposes of developing key risk indicators (KRIs).
- If no direct information is readily available, look at the metrics currently used (often in the form of key performance indicators [KPIs]) to determine whether they might be relevant lead or lag indicators.
- With respect to the risks for which more data gathering is not feasible and substitute measures are not available, consider alternative risk responses (such as avoid or share).
- Make sure relevant data sources are aggregated to provide useful information to understand the complete enterprisewide picture.
- Communicate frequently on risks that are difficult to quantify and for which outcomes cannot be predicted with confidence.

Remember: Even if the initial efforts to quantify a critical risk are crude at best, the improved understanding and resulting communications around the risk more than justify the effort. The qualitative assessment side of risk management is important, and we believe that it is likely to take on more significance in the aftermath of the global financial crisis.

Failure No. 7: Accepting a Lack of Transparency in High-Risk Areas

Lack of information for decision-making leaves management with little insight as to what is really happening or is likely to happen. Transaction complexity and volatility can further complicate efforts to understand the full picture when making decisions. If this environment exists within the organization – and management does not seek to correct the situation – that is a warning sign. Dysfunctional, excessive risk taking is fostered by an inability to see the full picture. When the sun shines on this behavior and management and the board can discuss it out in the open, the best decisions result. It is vital that executive management create risk awareness and an open, positive culture with respect to risk and risk management across the enterprise so that they and members of the board understand all aspects of how a firm's business model works and the inherent risks. Such an environment can only flourish when individuals can raise issues without fear of retribution to their compensation and careers.

Key indicators include:

- Unexpected surprises occur from time to time as a result of previously unknown risks.
- Performance is evaluated after the fact, due to the lack of analytical tools and leading KPIs and KRIs.
- An enterprisewide risk view is inhibited due to a high level of decentralized decision-making, risk management silos and ineffective oversight.
- Directors desire greater transparency to size exposure to risk and are not getting it.

With respect to matters of enterprisewide importance, an ERM approach to managing risk often centralizes policy-setting and creates focus, discipline and control around improving risk management capabilities over time as the operating environment changes. Further, it establishes an environment where people can raise their hands and express issues with confidence that their careers or compensation will not be threatened. This kind of open, positive and risk-aware environment is not possible without the CEO's active encouragement and visible support. To establish and sustain such an environment, it helps to:

- Submit reports to executive management and the board about the largest risk exposures undertaken by different business units and activities, with commentary on the ones that are performing well and those that are not.
- Implement an enterprisewide risk assessment process linked to the entity's business strategy.
- Consider the entity's risk appetite when delineating unacceptable risk exposures.
- Establish accountability for the largest risk exposures through a clear policy structure and effectively designed procedures, metrics, measures and monitoring.

Failure No. 8: Not Integrating Risk Management with Strategy-Setting and Performance Management

Risk is often just an afterthought to the formulation of strategy, resulting in strategic objectives that may be unrealistic and risk management becoming an appendage to performance management. The consequences of this failure include a strategy the organization is unable to deliver, deteriorating competitive position, inability to adapt to a changing operating environment and loss of enterprise value that took years to build and will require years to restore.

Key potential indicators of this failure include:

- Poor alignment of risk responses with strategy and enterprise performance management
- No connectivity of risk management to core management processes
- No effort to anticipate risk scenarios that could derail execution of the strategy
- Unacceptable risk taking or unnecessary risk-averse activity

To avoid this failure, management should implement an integrated approach and discipline to deploy strategy and manage the associated risks. An approach to integrate strategy, performance and risk would:

- Proactively identify, source and mitigate the risks inherent in the strategy
- Communicate and deploy strategy in a consistent manner across the enterprise
- Provide real-time transparency into the operations of the enterprise
- Ensure seamless integration of strategic plans, risk management and performance management

Protiviti has published a white paper on this approach titled *Performance/Risk Integration Management Model – PRIM²: The Convergence of Enterprise Performance Management and Risk Management.* It is available at **www.protiviti.com/go/prim2**.

Failure No. 9: Ignoring the Dysfunctionalities and "Blind Spots" of the Organization's Culture

An organization's culture can have a huge impact on its ability to prevent the occurrence of unacceptable risk events and identify new and emerging risks in a changing operating environment. Openness, transparency and accountability are all topics companies should be considering in the current environment and improving continuously in the future. More important, firms should pay attention to the root causes of management's missing the warning signs that something is either wrong or isn't working, which objective parties see easily with the benefit of 20-20 hindsight.

Following are key indicators that organizational dysfunctionalities and blind spots may exist:

- Rewards for extreme entrepreneurial risk taking
- Pressure to achieve unrealistic targets, executive resistance to bad news and internal competition fostering a warrior culture
- Tolerance for obvious conflicts of interests
- Inadequate linkage between risk management and priority business issues
- Gaps and overlaps in risk management responsibilities

Cultural issues can be a significant – but manageable – challenge. First, ensure that neither entrepreneurial risk-taking activities nor control activities are too disproportionately strong relative to the other – make them equal partners. Second, insist on an open dialogue regarding risks and opportunities. Third, make it clear to everyone that violation of established policies and limits related to the largest risk exposures is subject to disciplinary action.

Finally, implement an effective escalation process to ensure that significant problems are recognized and addressed *before* they start.

Failure No. 10: Not Involving the Board in a Timely Manner

According to a recent survey, 80 percent of directors of U.S. financial services firms believe they could do more to reduce the chance of future industry instability.[1] In all industries, boards generally have not been involved in a timely manner on issues surrounding such matters as management's risk appetite and the risks inherent in the corporate strategy and business plan.

Key indicators of this issue include:

- The board is only engaged in occasional ad hoc treatment of risk and risk management.
- Management informs the board after the fact when significant risks are undertaken.
- Directors are not fully knowledgeable of the priority business risks facing the company.
- The organization's risk profile is rarely, if ever, discussed at the board level.

To ensure that directors are involved in a timely manner, management should periodically evaluate the operating environment to identify the existing and emerging risks, and the board should be involved in that process. Management should engage the board in a dialogue about taking on significant risks *before* commencing action. There also should be a periodic substantive board-level dialogue regarding management's appetite for risk and whether the organization's risk profile is consistent with it. The board also should be satisfied that management's strategy-setting process appropriately considers, in a robust manner, the risks inherent in the business model.

Finally, appropriate risk reporting should be directed to the board. Such reporting might include, among other things:

- A summary of the enterprise's *critical* risks, broken down by operating unit, geographic location and product group
- A summary of the top- and worst-performing investments and reasons why
- Value-at-risk reports to assess the sensitivity of existing portfolio positions to market rate changes beyond specified limits
- Results of stress tests to consider the exposure of earnings or cash flow to severe losses from extreme rate changes
- A summary of scenario analyses evaluating the impact of changes in other key variables beyond management's control (e.g., inflation, weather, competitor acts and supplier performance levels) on earnings, cash flow, capital and the business plan
- A report of emerging issues or risks that warrant executive attention

Summary

In summary, we have discussed 10 common areas where risk management fails and how to avoid them:

1. Poor governance and "tone at the top"
2. Reckless risk taking
3. Inability to implement enterprise risk management
4. Nonexistent, ineffective or inefficient risk assessment
5. Falling prey to a "herd mentality"
6. Misunderstanding the "If you can't measure it, you can't manage it!" mindset
7. Accepting a lack of transparency in high-risk areas
8. Not integrating risk management with strategy-setting and performance management
9. Ignoring the dysfunctionalities and "blind spots" of the organization's culture
10. Not involving the board in a timely manner

The key indicators and suggested steps for avoiding the above failures provide the basis for a diagnostic approach that the board and executive management can use to check the health and viability of their organization's risk management.

[1] Survey taken between September 22 and October 4, 2008 at the 2008 PricewaterhouseCoopers Financial Services Audit Committee Forum, involving more than 300 board members, two-thirds of whom sit on the audit committee of financial institutions.