corporate compliance insights

Reimagining Risk:

An integrated approach to Enterprise Risk Management

Jim DeLoach

Introduction

There are four articles included in this e-book. The first addresses four themes for implementing enterprise risk management (ERM). At Protiviti, when we talk with executives about this topic, we often hear two questions: "Where do we start?" and "What do we do differently?" These two questions demand a pragmatic response, and in order to provide that response, there are four key themes we typically talk through.

These themes represent the crucial elements executives should be exploring when evaluating the role and effectiveness of risk management within an organization. They also provide context for directors when focusing their risk oversight. ERM is not a one-size-fits-all solution, and we have found that using these four themes as a design framework leads to a customized approach to improving risk management infrastructure.

One of the most important themes is integration, or embedding risk management within core management processes. Integrating risk management across the organization helps instill greater confidence with the board, CEO and executive management that the organization will be successful in achieving its objectives and larger corporate strategy.

Two articles dealing with relevant aspects of integration are included in this e-book: (1) defining organizational risk appetite, as part of integrating risk with strategy-setting, and (2) integrating risk within business planning. Both provide sensible approaches to encouraging the risk appetite dialogue between executive management and the board as well as making business plans more robust.

In the fourth e-book article, we focus on how to make the board's risk oversight process work. Since the financial crisis, boards have been more concerned with getting the risk oversight process right. In recent years, Protiviti, alongside the Committee of Sponsoring Organizations (COSO), conducted a comprehensive survey on the state of board risk oversight involving more than 200 active directors from a variety of industries. This article summarizes the five recommendations arising from this study.

We would like to extend a special thanks to Maurice Gilbert and CCI for compiling these previously published articles. Maurice and I hope you find these articles useful, as they remain relevant today. We hope you can take away one or two of the ideas presented in this e-Book and use them to improve your own risk management and oversight capabilities.

I. Integrating Risk With Strategy-Setting: Defining Risk Appetite

When integrating risk with strategy-setting, management should consider two things – risk appetite and an assessment of strategic risks.

Risk appetite is the mutual understanding between executive management and the board of directors regarding the drivers of, and parameters around, opportunity-seeking behavior. It is a high-level view of how much risk the entity is willing to take. Said another way, it is the aggregate of the acceptable level of volatility or variance in the company's operations and may be expressed in terms of its major lines of business.

Many see risk appetite as a highly theoretical concept that is difficult to apply in practice. Some people waste time looking for some magical metric, as if seeking the Holy Grail. Others wonder how to drive risk appetite down into the organization, which is a separate and different conversation around setting risk tolerances and is tied to the process of defining key metrics and targets. Some fail to grasp that risk appetite is an ongoing, dynamic dialogue rather than a one-time determination to be filed away until the next risk assessment.

Because risk appetite is inextricably tied to strategy-setting, neither is cast in stone. Finally, some fail to understand that their organization already has a risk appetite, whether they choose to articulate it explicitly or not. Management and the board take actions every day that reflect the organization's risk appetite. The real question is whether a mutual understanding exists between the board of directors and management as to what it is.

A risk appetite statement provides a directional tool pointing to the appropriate levels of enterprise risk. Prudence and common sense are vital when evaluating risk appetite over time. As risk levels and uncertainty change significantly, how does the new environment pair up with the company's risk appetite?

We believe that a risk appetite statement is a summary of observations, which we call "assertions," around relevant parameters that, taken together, frame the organization's appetite for risk. There are three key elements of a framework for framing these assertions:

1. **Articulate the risks that are acceptable or on-strategy that the organization intends to take because the risk taken is sufficiently compensated.**

   These risks are related to the strategic bets management makes to fuel growth in new markets, e.g., invest in the BRIC countries (Brazil, Russia,

India and China), build new plants to increase productive capacity, hire more people to augment the workforce and invest in new, innovative capabilities. These bets are presumed acceptable because management and the board typically determine that there is a satisfactory risk-reward balance, i.e., the upside potential for attractive returns warrants accepting the downside exposure.

2. **Articulate the risks that are undesirable or off-strategy that should be avoided and for which zero/minimal tolerances should be set**.

   These risks are ones for which the board and management have no appetite to assume. Policy prohibitions are often established for these risks to clarify management's strategic intent to avoid them, e.g., minimum standards for dealing with foreign officials, no appetite to invest in certain high-risk countries, avoidance of certain lines of business or restrictions on the use of financial derivatives for profit-making purposes.

3. **Define strategic, financial and operational parameters to provide a framework within which the company's risks are undertaken.**

   Parameters impact decision-making during the planning cycle and as strategic priorities and the business plan are executed. They drive discussions between executive management and the board when unforeseen opportunities arise or the parameters have been overstepped. Parameters may be expressed as targets, ranges, floors or ceilings and provide a context for establishing risk tolerances and limit structures. For example:

   1. **Strategic risk parameters** include new products to pursue and avoid and the investment pool for capital expenditures, hiring plans and expected M&A activity.

   2. **Financial risk parameters** include the maximum acceptable level of loss or performance variation including EPS variability, FCF growth/margin, EBIT growth/margin, target debt rating, target EBIT/interest coverage ratio and derivative counterparty criteria.

   3. **Operating risk parameters** include minimum capacity utilization, desired sustainability response, R&D investment pool, environmental requirements, safety targets, quality targets, and customer criteria and concentrations.

The three elements of the above framework provide a pathway for defining relevant risk appetite assertions that clarify for management, the board of

directors and other stakeholders within the organization the risks the enterprise is intent on taking and the parameters within which those risks are taken.

II. Integrating Risk with Business Planning

While some may use the two terms interchangeably to describe the same process, "business planning" is distinguished from "strategy setting" in two fundamental ways.

First, strategy setting establishes the enterprise's overall strategic direction, differentiating capabilities and required infrastructure to make those capabilities a reality, whereas a business plan lays out how the company intends to execute its strategy.

Second, the business plan is often developed in the context of a shorter time horizon (say, one year or the operating cycle, if longer) than a longer-term strategy. Some companies have a rolling multiyear business plan (three years, for example) that takes on the appearance of a continuous strategy update. Our focus here concerns a shorter-term business plan, such as an annual plan driven by the budgeting and forecasting processes.

In a business plan, it is critical to define the inherent soft spots, loss drivers and incongruities that could dramatically affect performance and adversely impact execution. In addition, the budgeting and forecasting processes supporting the business plan must be effective in managing liquidity risk to ensure the organization's solvency.

With respect to the selected business planning horizon, ensuring that the plan itself can be delivered according to expectations and that the company won't run out of money as it executes the plan (liquidity risk) are the two primary risks that really matter.

With respect to liquidity risk, there are a number of areas to consider. For example, there are the normal seasonal fluctuations, the inevitable unexpected developments causing revenue declines and operating cost increases, and the issue of inadequate financing facilities or poor working capital and/or cash flow management processes.

Then there are the unexpected events causing business disruption and exposing the company's failure to match the maturity profile of debts to the ultimate realization of the assets they are funding. Finally, there are the extraordinary circumstances leading to unplanned capital expenditures or breaches of loan

covenants. All of these areas point to the need for reliable budgeting and forecasting processes in which management and the board have complete confidence.

Every business plan should identify the appropriate metrics and measures to monitor. If the strategy-setting process contributes to an understanding of the risks inherent in the strategy, that understanding provides inputs to the determination of key metrics and targets. *It is at this point where risk management begins to intersect with performance management.* In effect, traditional key performance indicators (KPIs) and key risk indicators (KRIs) should converge to create a single family of metrics to drive the planning process.

While KPIs monitor progress toward the achievement of the strategy and are the primary means for communicating business results across the organization, KRIs provide lead and lag indicators of critical risk scenarios, resulting in a more balanced mix of forward-looking indicators to complement the usual KPI metrics around customer and employee satisfaction, quality, innovation, time and financial performance. For example, accumulated deferred maintenance in a manufacturing plant or refinery may be a lead indicator of environmental, health and safety risk.

Together, KPIs and KRIs provide direction around what should be managed in the execution of the business plan. The metrics selected must enable the organization to track progress toward the achievement of strategic objectives, monitoring and mitigation of risks, and compliance with internal policies, external laws and regulations. They supply the foundation for integrated business planning to provide a comprehensive framework to deploy and execute corporate strategy across an organization in concert with risk mitigation planning, budgeting, forecasting, resource allocation and the reward system. In many organizations, these are separate, individual processes, often championed by different parts of the organization.

An effectively integrated business plan does several things:

1. It describes the steps required to achieve strategic objectives and reach the targeted levels of success, and cascades the strategy down through the organization by decomposing it into performance plans that are supported by specific policies (including limits), procedures and integrated metrics to establish management accountability for results.

2. It links supporting budgets, KPIs and KRIs with performance expectations.

3. It focuses resource allocation on meeting the organization's overall strategic needs while managing risks within the entity's risk appetite.

4. It links the reward system to performance expectations through a compensation structure that is adjusted for risk and is fair to both the executives in question and the shareholders.

In summary, integrated business planning deploys the strategy at the level of greatest achievability and accountability, engages the appropriate managers who can access the resources required to get the job done, and incorporates risk capabilities (policies, processes, reports and systems) needed to address critical risks inherent in the plan.

III. Making Board Risk Oversight Work

Board risk oversight is an important aspect of ERM. In a comprehensive survey conducted by Protiviti, sponsored by the Committee of Sponsoring Organizations (COSO) and released in December 2010, more than 200 directors from a variety of industries provided insights regarding the current state of board risk oversight and how it can be improved.

Following are five recommendations arising from this study.

1. Implement a more structured process for monitoring and reporting critical enterprise risks and emerging risks to the board.

While most companies monitor and report on their risks, the survey results suggest the process can be improved. For example, a company might formalize a risk-assessment methodology based on appropriate criteria by making it a regular, more robust process with results shared with the board periodically.
Another approach might be to consider the unique characteristics of different categories of risks a company faces by using appropriate analytical frameworks. These could then feed an overarching process to develop a risk profile, merging the top risks into the vital few "critical enterprise risks." Those are two ideas. There are others.

2. Look for opportunities to enhance the risk reporting process and increase the regularity of reporting according to the organization's operations and risk profile.

According to the survey results, the most common types of risk reporting received at least annually by boards include: a high-level summary of top risks for the enterprise as a whole and its operating units; a periodic overview of management's methodologies used to assess, prioritize and measure risk; and a summary of emerging risks that warrant board attention.

The reporting most participants indicated were **not** received at least annually include: scenario analyses evaluating the effect of changes in key external variables impacting the organization; a summary of exceptions to management's established policies or limits for key risks; and a summary of significant gaps in capabilities for managing key risks and the status of initiatives to address those gaps.

3. Come to an agreement with management on the risk-related matters that need to be escalated to the board, addressing the what, when and why.

It is vital to the risk oversight process to determine what needs to be escalated to the board (e.g., limits violations, policy breeches, near misses, etc.) as well as when and why (e.g., the potential board inquiries and actions).

4. Encourage techniques that foster out-of-box, big-picture thinking focused on the critical assumptions underlying the corporate strategy to assess strategic uncertainties the enterprise faces.

The survey results found that less than 15 percent of respondents noted that the board is fully satisfied with the processes for understanding and challenging assumptions and inherent risks associated with the corporate strategy and monitoring the impact of changes in the environment on the strategy.

Given the riskiness and volatility of the times, organizations may want to focus on whether developments in the business environment have resulted in a disruptive change affecting these critical underlying assumptions and inherent risks and the effects of such change on the organization's business model. This focus may assist the board in addressing two questions that are fundamental to the risk oversight process: "What do we do if the critical assumptions underlying our strategy are no longer valid?" and "How would we know if our assumptions are no longer valid?"

5. Initiate and sustain a risk appetite dialogue between the board and management with a defined process, and ensure the results of this dialogue are driven down into the organization in an appropriate manner.

Given that risk levels and uncertainty have changed significantly over recent years for most organizations, the board and management may find it beneficial to engage in a periodic dialogue on risk appetite. This dialogue could cover such topics as the maximum acceptable level of performance variability in specific operating areas; targeted operating parameters; upside/downside debates on significant matters; the risks and assumptions inherent in the corporate strategy; the "hard spots" and "soft spots" in the business plan; and the implications of changes in the operating environment on the core assumptions inherent in the strategy, including the desired appetite for risk.

The board also may want to consider when and under what circumstances it should be informed of exceptions and near misses to the organization's risk tolerance parameters and any planned actions to address them through policy and process improvements.

The above can be applied to most organizations and would augment the enterprise's ERM process, irrespective of how the board chooses to organize itself for risk oversight.

IV. Four Themes for Implementing ERM

When discussing ERM and how to improve the value it adds to the enterprise, executive management and directors often ask, "Where do we start?" At the heart of this question is the desire for a simple and pragmatic point of view that makes sense in practice.

For many companies, risk management has focused on protecting the tangible assets reported on a company's balance sheet and the related contractual rights and obligations. Traditionally, this means the placement of insurance, management of treasury risks, mitigation of environmental issues, and elimination of health and safety risks in the workplace, among other things. While this traditional role has served a useful purpose in the past and should continue to function, the question arises as to whether risk management can and should serve a higher and better use.

While there is no one-size-fits-all, there are four foundational elements that frame what executive management and directors need to consider when implementing ERM. These elements are intended to be flexible in application, which is essential because risk profiles vary in complexity across industries. The four elements are discussed below.

1. Process

Like other worthwhile activities in a business, risk management requires a process. As with any process, there needs to be a purpose, inputs, activities and outputs. The activities of the risk management process typically include the identification, sourcing, measurement, evaluation, mitigation and monitoring of risk.

The purpose of the process varies from company to company. One company may seek to reduce risk or performance variability to an acceptable level. Another may seek to prevent unwanted surprises. Still another company may seek to facilitate taking more risk in the pursuit of value creation opportunities. Regarding the process, there is a large body of knowledge that is readily available for companies to adapt to a point of view that fits their circumstances.

2. Integration

The relevance of the risk management process increases if it is integrated with core management processes. The idea is to integrate risk management with what matters to instill in the board, CEO and executive management greater confidence that the organization will be successful in achieving its objectives and executing its strategy.

The nature and extent of integration vary from industry to industry and company to company, and are highly dependent on management's operating style. The scope of integration could include one or more of such core management processes and activities as strategy setting; annual business planning; performance management; budgeting; capital expenditure funding; and M&A targeting, due diligence and integration. Effective integration can result in risk management becoming more integrated with the rhythm of the business so that it can make value-added contributions to establishing sustainable competitive advantage and improving business performance.

3. Culture

Even the most well intentioned risk management process can be compromised if dysfunctional organizational behavior exists and is allowed to fester. If the CEO is not willing to pay attention to the warning signs posted by the risk management function, if the reward system is not sufficiently balanced with the long-term interests of shareholders, if the board is not asking tough questions about the assumptions and risks underlying the strategy, or if risk management is so mired in the minutiae of compliance that it is not focused sufficiently on strategic issues, risk management will likely not have an impact at the crucial moment when a contrarian voice is needed.

A culture that is conducive to effective risk management often encourages such things as open communication, sharing of knowledge and best practices, continuous process improvement, and a strong commitment to ethical and responsible business behavior.

4. Infrastructure

Given the nature of the organization's risk management process, the core management activities with which that process is integrated, and the strengths and weaknesses of the organization's culture, we can now ask the following question: Is the organization's existing infrastructure sufficient to get the job done?

By infrastructure, we mean the company's policies, internal activities, organization, reporting and systems related to managing risk. If the answer is "yes," then we move on. If the answer is "no," the next question becomes: What changes are needed?

Changes could include any combination of things, including a risk management policy, more explicit dialogue around risk appetite, a risk management committee, a chief risk officer, improved risk reporting, and more reliable systems and data.

These four elements define what executives should be looking at when evaluating the role and effectiveness of risk management within the organization.

ABOUT THE AUTHOR

Jim DeLoach has more than 35 years of experience and is a member of the Protiviti Solutions Leadership Team. His market focus is on helping organizations succeed in responding to government mandates, shareholder demands and a changing business environment in a cost-effective and sustainable manner that reduces risk to an acceptable level. He also assists companies with integrating risk management with strategy setting and performance management. Jim also serves as a member of Protiviti's Executive Council to the CEO.