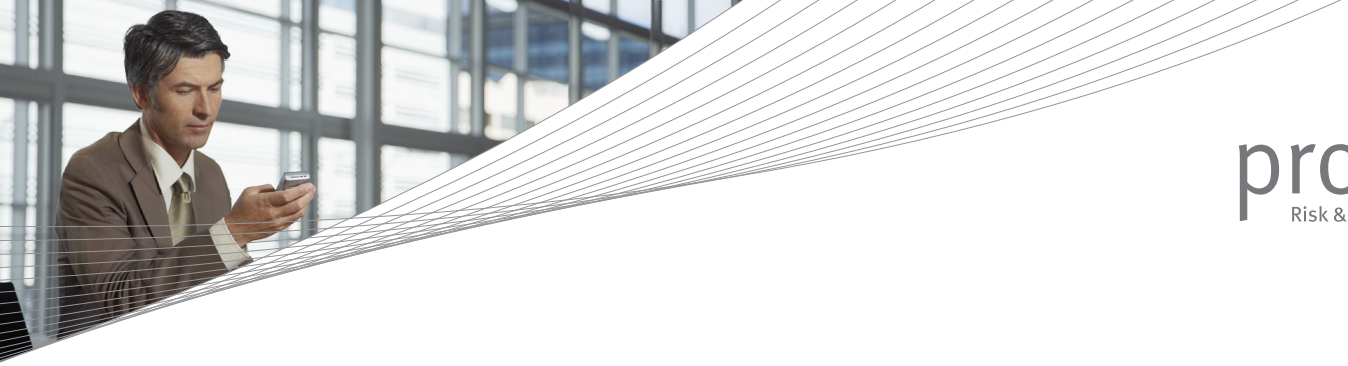

protiviti®
Risk & Business Consulting.
Internal Audit.

The Bulletin

Volume 4, Issue 3

Making Your Risk Assessments Count: An Operational and a Compliance Perspective

In the previous issue of *The Bulletin,* we noted that it is common practice for organizations to base their traditional risk assessment approaches on subjective inputs of the severity of impact from potential future events and their likelihood of occurrence. We also suggested several reasons why companies find it challenging to move beyond a risk assessment to actionable steps that can be incorporated into a business plan. And we provided a strategic perspective to assessing risk that was driven by the unique characteristics of strategic uncertainties. Now, we will consider an operational and a compliance perspective to making your risk assessments count.

Consider the distinguishing characteristics of risk

Traditional assessment approaches often do not address the unique characteristics of the risks a company faces. While using a common analytical framework to evaluate risks with different characteristics may make the assessment process easier to execute, it also may not be as effective as approaches that could provide more insight into how to respond to assessed risks.

Risks have well-known similarities; that is, all risks present a potential impact on an organization, and management does not know if or when they will transpire. In a risk assessment, there also are important and distinguishing differences among major categories of risk that should be considered. For this discussion, we will segregate risks into the following broad categories:

- **Strategic** – The risk that the business model is not effectively aligned with the strategy or that one or more future events may invalidate fundamental assumptions underlying the strategy. These risks relate primarily to the external environment (e.g., the actions of competitors, changing customer wants, technological innovation and the actions of regulators). We illustrated two approaches to assessing these risks in the previous issue of *The Bulletin*.
- **Operational** – The risk of one or more future events impairing the effectiveness or viability of the business model in creating value for customers and achieving expected financial results. These risks relate to the various business activities along the value chain within which the organization's business model is applied (e.g., the supply chain, customer fulfillment processes, human resources, information technology, key channels, key customers and end users).
- **Financial** – The risk that cash flows and financial risks are not managed cost-effectively to (a) maximize cash availability and preserve liquidity, (b) reduce uncertainty of currency, interest rate, credit, counterparty and other financial risks, or (c) move cash funds quickly and without loss of value and at minimal cost to wherever they are needed most.
- **Compliance** – The risk of noncompliance with laws, regulations, internal policies and/or contractual arrangements resulting in penalties, fines, increased costs, lost revenue and/or reputation loss. Financial reporting is a form of compliance risk for public companies.

There are different ways to distinguish these four categories of risk. First, there is ***susceptibility to measurement***. The above categories of risk are not subject to the same level of precision from a quantification standpoint. Strategic risks, as defined above, arise primarily from invalid assumptions and a lack of alignment in execution. Given their nature, the analytical framework applied to these risks must be more qualitative than for other risks.

For example, interest rate and other price risks are easier to size in terms of their impact on the business by using scenario analyses, stress tests and value-at-risk frameworks that take into account changes in the economy and market volatility. Strategic risks arising from invalid assumptions, on the other hand, are more about obtaining sufficient knowledge of expected economic trends, competitors, customers, suppliers, regulators and other external environmental factors to evaluate whether the critical assumptions underlying the strategy remain valid.

Second, there is ***time horizon***, the period of time over which management assesses the level of risk and the alternatives for managing risk. The longer the assessment horizon, the more likely a stated scenario or event could occur. Because they are a function of the board's and executive management's long-term view of the market and the expected pace of change, strategic risks have a longer time horizon than

other risks. By contrast, operational risks typically have a shorter horizon, as they are often evaluated in the context of the business planning cycle. For instance, one company's board requested that management conduct two risk assessments: one for one year, to mirror the horizon for the annual budget, and the other for three years, to mirror the horizon for the strategic plan. The time horizon can be a significant factor in determining the currency of the organization's risk assessment in a rapidly changing environment. The time horizon also can have an impact on management's risk response options. For example, some issues, such as a capacity shortage at a manufacturing company, can be quite severe over the short term. However, most risks, including capacity, are less of an issue over the longer term because management has more flexibility to make adjustments.

The appropriate risk assessment approach applied to operational risks suggests the need for an end-to-end, extended enterprise view of the value chain.

Third, ***variability in outcomes*** suggests that exposure to risk can result in either upside or downside consequences. Compensated risks are two-sided and present potential for upside (i.e., if we were to list all foreseeable future outcomes arising from the risk, including an estimate of the net cash flows relating to each possible outcome discounted to their present values, we would have a range of outcomes with both net positive and net negative cash flow results, giving rise to performance variability). Because an effective strategy is about pursuing the best bets in the context of the enterprise's risk/reward balance, compensated risks are often inseparable from the execution of the enterprise's strategy. The risks are compensated because the potential for upside is sufficient to warrant accepting the downside exposure.

The risks associated with initiating operations in new markets, introducing new products, or undertaking large research and development projects are common examples of these risks. By contrast, uncompensated risks are one-sided because they offer the potential for downside with little or no upside potential (i.e., every foreseeable future outcome results in net cash outflows, creating a loss exposure). Uncompensated risks would, for example, include environmental, health and safety risks where there is very little, if any, upside over the long term to cutting corners and taking shortcuts that accumulate and create unacceptable risks.

Finally, there is ***nature of response***. A decision to accept a risk can lead to a conclusion that the risk should be retained, reduced or exploited. A decision to reject a risk can lead to a conclusion to avoid it altogether or transfer it to an independent, financially capable third party. There is a "decision tree" of sorts around evaluating how to respond to a risk; this decision tree is navigated differently depending on the nature of the risk. For example, compliance risks are often managed through policies and procedures designed to reduce the risks to an acceptable level. Strategic risks, however, may arise from uncertainties requiring ongoing monitoring of the environment to ensure strategic assumptions remain valid over time. Operational risks may require better alignment of processes along the value chain or the development of rapid response plans in the event a critical component of the value chain, such as a key supplier, is lost.

Once we recognize that the four categories of risk – strategic, operational, financial and compliance – vary according to their distinguishing characteristics, it becomes clearer why the analytical frameworks used to assess each category should be designed to consider those unique characteristics.

An operational perspective to risk assessment

Often, an operational assessment is directed to assessing performance against quality, time, innovation and cost targets to identify gaps in process performance. Significant performance gaps lead to decisions around making appropriate midcourse corrections or analyzing root causes with the objective of determining actionable process improvements to close the gaps. Given this traditional approach to an operational review, the question arises as to the appropriate level of focus when evaluating operational risks.

The reality of today's business environment is that the enterprise is boundaryless and not an island. Accordingly, the appropriate risk assessment approach applied to operational risks suggests the need for an end-to-end, extended enterprise view of the value chain, requiring consideration of looking upstream to supplier relationships, including strategic suppliers, as well as downstream to channels, customer relationships and the ultimate end users.

For instance, a consumer packaging company serves the needs of consumer products companies in marketing their products to their customers. The marketing strategies of its customers, as well as the preferences of the ultimate consumers, can have a significant impact on demand for the company's packaging products. In effect, the enterprise's business relationships are just as important to its success as its internal processes, personnel and systems because they are inextricably linked to what makes the business model work. Therefore, the assessment of operational risk is directed to understanding the risk of loss to, or ineffective performance of, any of the key links in the chain. By contrast, a "four walls"-oriented approach to evaluating operational risks that focuses solely on the company's internal processes and systems risks misses the big picture.

What would happen to the organization's business model if any key component of the value chain were (a) taken away through either failure or an unexpected catastrophic loss or (b) altered in a significant way to place the company at a strategic disadvantage? To illustrate the use of an "extended end-to-end enterprise" perspective, the analytical focus is

on the entire value chain and the company's positioning within the chain. For example, which suppliers do we depend on for essential inputs? Suppliers' inputs include raw materials, component parts and supplies, as well as the transportation for delivering them to the company's facilities in a timely manner. Questions that can arise when evaluating suppliers' inputs include:

- Are we confident that strategic suppliers meet specifications?
- What if one or more strategic suppliers were lost?
- What if there were temporary shortages in raw materials?
- What if there were serious defects in supplier inputs?
- What if there were significant disruptions in transportation?
- What if one or more of the above events caused material volatility in costs?

Likelihood of occurrence may not be as significant a factor in evaluating exposure to catastrophic events as the enterprise's response readiness.

Will the company's key suppliers take corrective action in the event of a disaster? Is there a formalized understanding and agreement in place? One company had a major supplier decide to discontinue the manufacture of key component parts for its products, and the company had to take this production process in-house in order to continue doing business.

Other inputs include the available labor force and talent pool, the availability of power at a reasonable price, lines of credit and working capital. With respect to company processes, there are other considerations. For example, there are high-value employees on whom the company truly depends; critical processes, systems and facilities; and key outputs, products and services. In addition, the company's products and services are distributed through channels to major customers, and there are transportation and logistics considerations.

What would happen if any of these elements of the value chain were taken away? Said another way, at every stage of the value creation process, what would be the implications of a shortage, disruption or quality problem in an input or output? How long would the company be able to operate? What if major customers were to fail? What if vital customer contracts were not renewed? What if key customers were to consolidate? What if weather patterns adversely affected customer demand? What would be the impact on the business?

When evaluating operational risks, management should consider the following factors:

- The velocity or speed to impact, including whether the loss of any critical component of the value chain can occur without warning (i.e., does it smolder or is it sudden?)
- The persistence of the impact (i.e., the expected duration of time before the loss of the component can be replaced)
- The resiliency of the company in responding to a catastrophic event
- The extent of uncompensated risks the company faces across the value chain (e.g., increased warranty costs and/or product recalls or the potential for increased environmental, health and safety exposures)

These issues should be considered periodically when conducting operational reviews. In this analysis, note that while the likelihood of occurrence can be a consideration, it may not be as significant a factor in evaluating exposure to catastrophic events as the enterprise's response readiness. Sooner or later, every company faces a crisis. Even the most effective risk management cannot prevent this exposure.

Just as a crisis is a severe manifestation of risk, crisis management is the natural follow-on to risk management. A rapid response to sudden, unexpected events depends upon the enterprise's crisis management capabilities. Fires cannot be fought with a committee. Building a capable crisis management capability is a management imperative for risks with a high velocity to a severe reputation impact. A world-class response to a persistent crisis is vital to the company's ultimate recovery from it. Risk assessments focused on velocity to impact, the persistence of the impact, and response readiness can help identify areas where preparedness is more critical.

For compliance risks, in lieu of mindless guesswork on probabilities, consider the effects of noncompliance in terms of the impact on reputation, the velocity or speed to impact, the persistence of the impact, and the enterprise's response readiness.

A compliance perspective to risk assessment

The traditional approach for assessing compliance risks focuses on severity of impact and likelihood of occurrence, often on a residual risk basis. This approach often results in a cluster of low likelihood risks with varying levels of potential severity, and fails to address the potential implications to the enterprise of a breakdown in established policies and procedures. For compliance risks, as we defined them earlier, in lieu of mindless guesswork on probabilities, companies should consider the effects of noncompliance events in terms of the following factors:

- The impact on reputation (e.g., fines, penalties, loss of revenues, legal fees and other costs, loss of market capitalization, the "spotlight attraction" effect)
- The velocity or speed to impact, including whether the effects of noncompliance can occur without warning and how quickly the effects can escalate, attracting media and regulatory attention
- The persistence of the impact (i.e., the duration of time over which the noncompliance event will affect the company)

- The enterprise's response readiness (i.e., how resilient the company is in responding to a noncompliance event)

As with operational risks, the "no boundaries" view of the enterprise can have an impact on compliance risks. For example, lead content, toxic materials, impure ingredients and other inputs provided by suppliers that do not meet specifications aligned with the laws and regulations to which the company is subject can damage the company's brand and reputation in the market, regardless of the suppliers' culpability. While compliance risk management addresses applicable laws and regulations rather than the effects of market forces or customer behavior, many of the same forces that drive other risk categories have an impact on compliance risk. Personnel attrition, influx of new personnel, rapid growth, new technology, increased complexity, speed to market and other performance pressures, for example, can create an environment in which compliance issues can arise. So, too, can the business customs of different countries, new lines of business, new acquisitions and corporate restructuring.

Financial reporting risks, a variant of compliance risks, are a separate conversation. Given the structure provided by the Sarbanes-Oxley Act compliance process in the United States and similar processes in other countries, most companies understand that these risks, and the related internal control environment, require a separate assessment framework that focuses on financial reporting assertions.

Engage the appropriate process owners to drive expected results

For operational and financial risks, the expected results from assessing risk include:

- Monitoring performance
- Evaluating and implementing midcourse corrections
- Determining areas where response plans are needed
- Implementing process improvements to improve performance
- Providing inputs into the business planning process and periodic operational reviews

For compliance and financial reporting risks, the expected results include identifying, evaluating and remediating deficiencies in the control environment.

Responsibilities for the assessments of these categories of risks, as well as the responses to those assessments, can be allocated to the operating units, finance function, general counsel, chief compliance officer (if there is one), other support functions, and the risk committee and/or senior risk officer (if there is one), according to the nature of the risks. The internal audit function can play a supportive or consultative role, as appropriate. The idea is to engage the managers best positioned to own the risk assessments, as well as the appropriate follow-on activities to act on the assessment results.

What about financial risks?

In Issue 2 of *The Bulletin*, we considered an analytical framework for strategic risks. In this issue, we considered frameworks for operational and compliance risks. With respect to financial risks, companies use a variety of techniques to assess them, including forecasts, modeling, scenario planning, value-at-risk frameworks, and assessments of exposure of financial and physical assets and sustained operations to hazards. The wide-ranging nature of these tools is a topic that is beyond the scope of this discussion.

Summary

The point of our discussion in this and the previous issue of *The Bulletin* is that subjecting all risks to the same analytical framework is not the most efficient and effective approach to integrating risk management with the core management processes of the business. In our view, an enterprise risk management process does not envision that all risks be subject to the same assessment methodology. We suggest that robust approaches applied to different risk categories according to the underlying characteristics of risks are needed to identify the top risks of those categories. Those approaches then would feed an overarching process that management uses to develop a risk profile, merging the top risks to summarize the vital few "critical enterprise risks" upon which management and the board should center their mutual focus. That process is yet another topic meriting further discussion.

About Protiviti

Protiviti (**www.protiviti.com**) is a global business consulting and internal audit firm composed of experts specializing in risk, advisory and transaction services. We help solve problems in finance and transactions, operations, technology, litigation, governance, risk, and compliance. Our highly trained, results-oriented professionals provide a unique perspective on a wide range of critical business issues for clients in the Americas, Asia-Pacific, Europe and the Middle East.

Protiviti has more than 60 locations worldwide and is a wholly owned subsidiary of Robert Half International Inc. (NYSE symbol: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

protiviti®
Risk & Business Consulting.
Internal Audit.