Risk Management: Beyond Compliance
by Bill Sharon

Executive Summary

- The boundaries between risk management and compliance have eroded over the past decade, to the detriment of both functions.
- The definition of risk should be expanded to include opportunities and uncertainties, not just hazards.
- The context for assessing operational risk is business strategy.
- The role of risk managers needs to expand so that they become coordinators of the risk information that is readily available in operational and business units.
- The perception of risk is dependent on one’s organizational responsibilities, and the convergence of those perceptions is the central focus of the management of risk.

Introduction

Over the past decade the line between risk management and compliance has been blurred to the point where, in many organizations, it is impossible to determine if they are not one and the same. In part, this confusion between the two functions was initiated and then exacerbated by the passage of the Sarbanes-Oxley Act of 2002 and the implementation of Basel II. Both of these events consumed a great deal of resources, and many consulting firms labeled these efforts “risk management.” They are, in fact, compliance requirements designed to protect stakeholders and, in the latter case, ensure the viability of the financial system. They are not designed for, and nor can their implementation achieve, the management of risk in individual companies or financial institutions.

This confusion between compliance and risk management has led to a defensive posture in dealing with the uncertainties of the competitive business environment. Risk has been confined to the analysis of what could go wrong rather than what needs to go right. Risk management organizations have become the arbiters of what constitutes risk and have assumed an adversarial relationship with business managers, particularly in capital allocation exercises. Failures and scandals are met with calls for more regulation, the implementation of regulations becomes the province of risk management organizations, and the execution of strategy (arguably the area in most need of risk management) becomes further separated from any kind of disciplined analysis.

An Expanded Definition of Risk

As Peter Bernstein tells us in his book *Against the Gods: The Remarkable Story of Risk*, the word risk comes from the old Italian *risicare*, which means “to dare.” Daring is the driving idea behind business, the idea that a product or a service can achieve excellence and value in the marketplace. Strategy necessarily incorporates risk from the perspective of those actions which are required for its success.

In 1996 Robert G. Eccles, a former Harvard Business School professor, and Lee Puschaver, a partner at Price Waterhouse (now PricewaterhouseCoopers), developed the concept of the “business risk continuum.” They argued that organizations that were successful in managing risk were those that focused on uncertainties and opportunities as much as they did on hazards. The context for evaluating risk in this manner is business strategy. This idea—that the definition of risk should be expanded to include those actions that an organization needed to embrace to achieve its goals—was revolutionary and codified what some companies were already beginning to initiate. Unfortunately, the narrow view of risk has prevailed for the past decade, and Eccles’ and Puschaver’s work has essentially been ignored.

The overwhelming emphasis of most risk organizations today is on the hazard end of the scale. Dot.com, Enron, and now subprime, along with the increased focus on terrorism, cataclysmic natural disasters, and the potential for pandemic diseases, have most complex organizations in a defensive posture. The problem with this approach is that risk driven from the hazard perspective is experienced as overhead in
the operational disciplines and business units; it’s a cost of business, not an activity that enhances value or improves the possibility of success.

By expanding the definition of risk (or returning to its original meaning) companies can harness the inherent risk management abilities and information available throughout their organization and develop a predictive process to address mission-critical tasks. Understanding how risk is perceived and how people react to those perceptions is an essential step in managing the opportunities and uncertainties inherent in implementing a business strategy.

Organizational Roles and the Perception of Risk

Daniel Kahneman and Amos Tversky, the authors of “Prospect Theory,” conducted a variety of experiments on the perception of risk and the responses that people had to identical information presented in different contexts. Among their conclusions they determined that:

1. emotion always overrides logic in the decision-making process,
2. people suffer from cognitive dysfunction in making decisions because they never have enough information,
3. people are not risk-averse, they are loss-averse.

While these conclusions may be unsettling to those involved in quantitative risk analysis, all three are useful assumptions around which to build a proactive risk management process. Emotion is at the core of any business—the desire to produce the best product, offer the best service, and compete in the marketplace comes from passion, not analytics. Managing risk is about managing emotion, not eliminating it.

From an organizational perspective, the perception of risk is colored by one’s responsibilities. In the operational environment, technologists see opportunities in deploying software and hardware. HR professionals define success as the attraction and retention of high-performance employees. In the business units, opportunities require risks to be taken in order to capture market share or evolve a product line to the next level. Often these business leaders are unaware of the operational capabilities and capacities on which they must rely to achieve their goals. Operational managers often lack clarity on the business models they support. Individually, these perceptions of risk tell only part of the story and require the balance of all of the organizational perceptions in order for the cognitive dissonance to be managed and mitigated.

In this context, risk managers become coordinators of business intelligence rather than arbiters of what is and is not a risk. The management of risk is a communication process that is central to the success of the enterprise rather than an overhead process that compliance so often becomes. Participation in risk management is equivalent to participating in the development of business strategy. The desire not to lose (rather than the misguided view of being averse to “daring”) is the underlying motivation for the process.
The Risk Perception Continuum

Figure 1. The risk perception continuum

The risk perception continuum (Figure 1) summarizes the categories of risk and how they can be placed in an operational context. Using Eccles and Puschaver’s concept of the three categories of risk, an organization can assign one of three different perceptions to determine the source and value of risk information:

- **What Should Be** is the perception of risk that comes from external standards. These are “best practices” for both operational and business managers. The measures involved determine the degree to which an organization is aligned with these practices in the context of what the organization wants to achieve. For example, alignment with “best practices” for a data center is likely to be more important for a financial institution than an advertising agency. It is tempting to place compliance functions in this area and track these issues as hazards. This is a mistake on two levels. First, the risk management process is central to the success of the organization and needs the oversight of the audit function. Putting them in the same unit creates a conflict of interest, one that is clearly identified in the Committee of Sponsoring Organization’s (COSO) enterprise risk management framework. Second, compliance is a legal and regulatory function. One does not assess the risk of not complying. The primary audiences for this information are regulators and external auditors, and the ability to adhere to these requirements is really the baseline for participating in the marketplace.

- **What Is** comprises the uncertainty of the operating environment of the organization. This is the area where quantitative analysis and hedging are done to determine the upside and downside of a deal. It is here that both business and operational managers have the greatest impact on the management of risk, and it is here that the communication of the different perceptions of risk is most critical. The convergence of these perceptions constitutes valuable business intelligence. The classic example of managing risk in this manner is the HR hiring process. The MD of equity trading in an investment bank may have an urgent need for a large number of junior traders. The human resources department has a responsibility to ensure that the people the MD wants to hire have actually attended the universities claimed on their resumés and that they have passed a strenuous background check.
check. The tension between these two perceptions is satisfied by the candidates signing a letter accepting their immediate dismissal should they be found to have misrepresented their qualifications. The organization embraces the risk that the contributions to the strategy will outweigh the potential for any damage that might be done during a relatively small window of time.

- What Could Be is the repository of the strategy of the organization and the perception of what risks need to be taken for it to be achieved. This perception is dynamic and responds to the demands of the marketplace, as well as the capabilities of the operating environment.

Perhaps the best known example of how strategy drives the management of risk in an organization is the behavior of the US space agency, NASA, following John F. Kennedy’s announcement that there would be an American on the moon by the end of the 1960s. In recently released tapes of meetings between Kennedy and James Webb, the director of NASA, the impact of strategy on operational capabilities is well illustrated. Webb advises Kennedy of the vagaries of space and the need to expand the space program to include a number of interim steps necessary to gain a better understanding before anyone can go to the moon. Kennedy listens and then tells Webb that he doesn’t care about space, he wants to get to the moon before the Russians.

What’s interesting about this exchange is that Kennedy was defining a strategic goal that had no near-term likelihood of being achieved. He was also using that strategic goal to redefine the risk. The technical risk was unknowable at the time, but the political risk was quantifiable. Strategy organizes the operational environment and focuses it in specific directions. It requires operational managers to converge their perceptions of risk with the goals of the organization.

Figure 2. Converging the perceptions of risk

Figure 1 also demonstrates the difference between driving risk management from the opportunity or strategy perspective as opposed to the hazard perspective. The latter approach tries to force standards up through the organization. Operational managers experience this as an audit process and, other than quarterly reports from the audit committee, very little of this information receives much attention from the senior executives responsible for implementing strategy.

Alternatively, risk management driven from the opportunity perspective creates a communications vehicle for the entire organization. This is a bi-directional process because, as the strategy is communicated into the operating environment, the organization responds with business intelligence.
Implementing a Risk Management Process

Using the organization’s strategy as the context (rather than “best practices” or regulatory requirements), the first step in the process is to ask operational managers to identify the risks that must be embraced in order to achieve this strategy (operational disciplines are defined as those organizational units that do not generate income, i.e. finance, HR, IT, PR, etc.). Once identified, these activities are assessed—usually using a RAG (red, amber, green) rating—to determine the likelihood of their being achieved.

There are two important steps in this first stage of the process that are often lacking in risk management programs.

1. Operational managers are asked to predict a risk rating, usually on a quarterly basis, for the next four quarters. This provides the organization with more valuable data than point-in-time risk assessments, whose shelf-life tends to be quite short. It also provides operational managers with the ability to communicate anticipated challenges in the future and/or illustrate how current challenges will be positively addressed over time.

2. Operational managers are also asked to note whether the activities they believe must be undertaken have sufficient funding. Once this information has been collated, the organization has a map of where it is investing in managing risks central to the strategy and where it is not.

Operational managers are then asked to complete an actual vs. planned assessment at the end of each quarter. This is not an exercise to assess competency, but rather another channel for communication in the risk management process. Strategy may change, requiring a new perception of risk. Operational awareness of greater or lesser challenges may impact the original risk rating. Departures from the original assessment are expected and should be viewed as business intelligence rather than as a scoring of prescient abilities.

Once the process is established with the operational managers, the second stage of the risk management process can be implemented. Here, business managers are asked to contribute their perceptions of risk to the mission-critical operational activities that have been identified. For example, if the IT department identified the rollout of a new operating system as a risk that needed to be embraced and rated it as an amber or a red given the exposure in maintenance and security, the business managers might rate it as a green as they have no clear knowledge of the technical issues. Differences in the perception of risk are expected and provide an opportunity to understand risk across operational and business disciplines.

The third stage (Figure 2) in the risk management process is the audit review, which not only validates the process itself, but also uses the risk assessments as a source for audit oversight of specific operational activities. The convergence of perception between operational and business managers and the audit function provides the risk management process with the widest possible range of understanding of risks to the strategy.

Once this process is established, metrics can be applied to risk ratings, operational disciplines can be weighted in importance by business unit, and portfolio views of risk can be developed across business units.

Case Study

JP Morgan—Managing the risk of outsourcing

The risk management process can be scaled to encompass the entire organization, a specific business unit, or a large project. A year prior to outsourcing 40% of its technology, JP Morgan initiated a predictive risk management program that converged the perceptions of technology and business managers and established an IT risk profile for each business unit.

- The IT self-assessment process was conducted quarterly on a global basis, and provided the bank with a portfolio view of IT operational risk across all business units.
- The risk profiles allowed the bank to negotiate service levels based on an understanding of where the internal IT group was supporting the business strategy and where improvements were necessary.
- The IT self-assessment process was transferred to the successful vendors and the business units continued to contribute their perceptions, resulting in a shared process between the vendors and the bank.
• Perhaps the most important result of the process was a better understanding in the business units of IT capabilities and capacities. The organization gained an understanding of the technology that provided competitive advantage (and should therefore be retained in the bank) and of the infrastructure and shared applications that could be turned over to external vendors.

Conclusion

No risk management function can ensure that negative events won’t happen. The complexity of the markets and the speed of change create exposures that are difficult to predict. Managing risk as a process that engages the entire enterprise in the achievement of the business strategy does, however, create a resilient organization that can better respond to difficulties that always arise.

Making It Happen

The operational risk management process described in this article begins with the business strategy but ultimately engages the entire organization. Senior management needs not only to endorse the process but also to participate in and use it on a continuing basis. The early stages of the process require patience, and some care should be taken in the initial implementation.

• There is often confusion in the operational disciplines about what is a risk to the business strategy and what is a best-practice or compliance requirement. Risk managers will likely need to assist operational managers in this distinction.
• Simplicity is key in the early stages of the risk management process. Many efforts collapse under their own weight when organizations attempt to accomplish too much in a short period of time. Risk management is about leveraging existing expertise; complex metrics can be applied once the system is robust.
• Using the risk management process as a communication process, not only for challenges but also for capacities and creative solutions, is essential in making it a robust vehicle for the generation of business intelligence.

More Info

Book:

Article:

Report:

Websites:
• COSO (Committee of Sponsoring Organizations of the Treadway Commission): www.coso.org
• Prospect theory: prospect-theory.behaviouralfinance.net and www.sjsu.edu/faculty/watkins/prospect.htm
• Risk Metrics: www.riskmetrics.com
• Strategic Operational Risk Management Solutions (SORMS): www.sorms.com

See Also

Best Practice
• The Effect of SOX on Internal Control, Risk Management, and Corporate Governance Best Practice
• Managing Operational Risks Using an All-Hazards Approach
• Risk—Perspectives and Common Sense Rules for Survival
• A Total Balance Sheet Approach to Financial Risk

Checklists
• Applying Stress-Testing to Operational Risk Exposure
• Basel II—Its Development and Aims
• Establishing a Framework for Assessing Risk
• Sarbanes–Oxley: Its Development and Aims

Thinkers
• Amos Tversky

Finance Library
• Mastering Risk, Volume 1: Concepts

To see this article on-line, please visit