Living With Risk

By Mukul Pareek, CISA, ACA, AICWA

While the term "risk management" may evoke thoughts of either the mundane job of managing insurance policies at one extreme or playing with complex derivatives on the other, it is in reality a part of every manager's job and should be recognized as such. An organizationwide recognition of the importance of risk management processes, tools and an omnipresent risk management culture is essential to maximizing shareholder value.

Risk and Reward

Profits are the reward for taking a risk. Risk and reward are positively correlated—the higher the risk accepted by a business, the higher the business's expectations of return. Management's job is to maximize shareholder value, which it does by seeking to generate the maximum possible level of return on capital employed given the risks resulting from operational and strategic business decisions. Considering an extreme hypothetical case, management can choose to accept no risk, invest the entire capital of the business in treasury bonds, and receive a risk-free return on shareholders' funds. In such a case, changes in enterprise value, the ultimate measure of shareholder value, will be limited to the market value of the bonds selected. If this hypothetical management team chooses to accept a higher level of risk, it could invest in higher risk bonds and obtain a higher yield that reflects the higher risk of default.

In other words, the risk decisions of the hypothetical management team would move it along the securities market line, or the risk-reward curve, and it would expect a greater reward for accepting higher risk. To accept a higher level of risk without corresponding returns would be suboptimum for management.

Much in the same way, everyday decisions that managers make commit their organizations to different levels of risk for which they must seek appropriate rewards. A conservative manager taking cautious decisions with low variability in outcomes can rightly expect a lower return from his/her decisions, while managers who take on above-normal levels of risk should be expected to generate more value for the organization. Management at all times should be aware of the risks to which its business is exposed so that it can demand the right returns from its operational managers and not place safe players on par with those who swing for the fences. Where possible, compensation schemes should recognize individual achievement on a risk-adjusted basis.

Figure 1 reflects the positive correlation between risk and reward. At zero levels of risk, only a minimal risk-free return on invested capital can be obtained. "X" reflects a suboptimal risk-reward payoff point where the business is earning a return less than what should be earned for the level of risk assumed; or, viewed from a risk perspective, the business has assumed risk for which it has not been compensated.

Management's risk management processes should allow senior executives to have a view of the risk assumed by the business at any given point in time and engage in a meaningful exercise to determine if any of their risk decisions are placing them at a suboptimum point on the risk-reward plane.

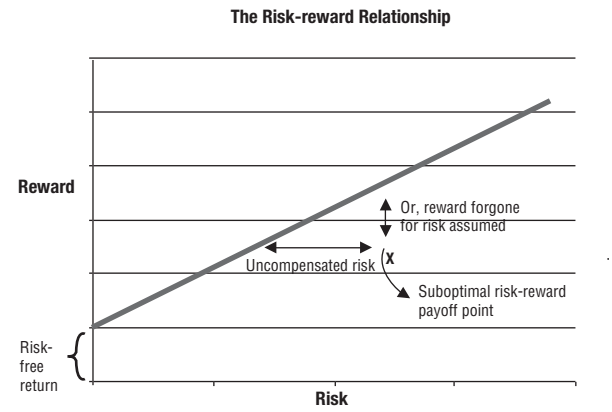
The Meaning of Value

Value means the total return to the shareholders (TRS) of a business. TRS includes two elements: dividends and changes in enterprise value.[1] Value created from the financial or operational decisions taken by the managers of a business is reflected in revenue increases, cost savings or release of locked-up capital—all of which are ultimately reflected in an increase or decrease in enterprise value. In practice, however, managers often measure the impact of their decisions by considering the impact on earnings. This is not inconsistent with the TRS view of value as earnings—either finance dividends or an accumulation as part of shareholders' funds—implying that changes in earnings change TRS by an identical amount.

Assuming that a higher risk posture without a corresponding increase in the rewards reduces value, being able to sustain the returns from the business while reducing risks increases value.

Management must always demand a higher return for higher risks taken; however, to be able to do that, it should be able to identify and assess the risks assumed.

Figure 1—Risk-reward Correlation



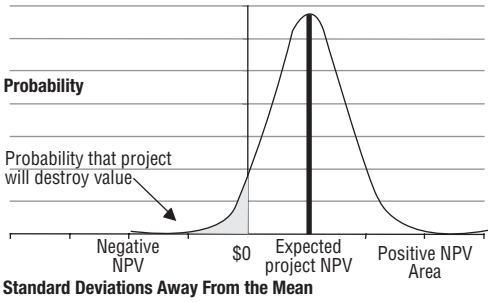
The Nature of Risk

Risk, according to financial theory, refers to volatility of outcomes. An important qualifier can be added to this perspective: while financial measures of risk, such as volatility and standard deviation, measure the upside and downside of deviations from expectations, only the downside variability is considered to be the true measure of risk, a view that is

aligned with the intuitive understanding of risk that most managers have.

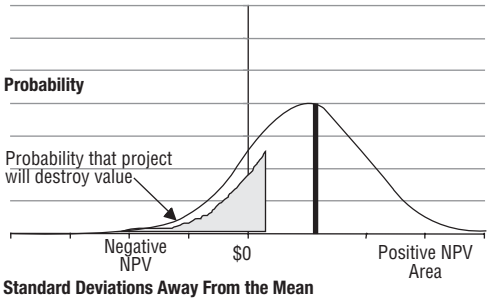
For example, consider a project undertaken by a manager with a given expected net present value (NPV) that reflects the project's contribution to shareholder value. However, the outcome of the project is not certain, and there is a risk that things may go wrong and actually reduce enterprise value. Assuming for a moment that project outcomes can be represented by a normal curve,[2] the potential distribution of actual NPVs at the end of the project is shown in **figures 2** and **3**.

Figure 2—Project's NPV Distribution: Low Volatility



Projects with low volatility have a significantly low downside risk when compared to a project with high volatility, though expected value is the same.

Figure 3—Project's NPV Distribution: High Volatility



Projects with high volatility have a significantly high downside risk when compared to a project with low volatility, though expected value is the same.

Managerial decisions—for example, whether to accept a project, as described previously—impact organizational risk in a similar way; they increase or decrease the overall risk of the organization by quantities that may appear insignificant in the larger context, but aggregate to determine the overall risk of the organization. This drives the organization either up or down the risk-reward curve. Investors rightly demand a greater return from organizations that take on greater risk and, given identical profits, place a smaller valuation (i.e., reduced TRS) on riskier companies.

Individual risks and exposures increase the variability of the TRS and, therefore, are inherently value destroying. However, this does not mean that management must cover every risk, but that being aware of the risks the business faces, management should make the right decisions that optimize shareholder value in line with a risk stance that is expected by its investors.

Should a Company Manage Risks?

It is occasionally argued that a company need not manage most risks because its shareholders can diversify their investments to corporations that are more aligned with their risk objectives. However, investors are poor bearers of organizational risk due to information asymmetries *vis-à-vis* the managers of the firm. It is the job of management and the board to proactively invest in managing risk and protect the wealth of the shareholders. That is why risk management is an important activity for all firms.

Types of Risk

Perhaps the most difficult aspect of managing risks is identifying risks. More things will happen in the future than can be predicted today, i.e., the problem of "unk-unks" (unknown unknowns). Even what can be anticipated today results in a list longer than what can be feasibly protected against. Therefore, it is essential to have a risk management process in place that identifies key unique risks to which the organization is subject, and to decide on an appropriate risk response that is the result of a conscious management decision rather than merely a hope to be a lucky bystander as the future unfolds.

The Basel II framework is a framework for determining capital adequacy requirements for financial institutions. In doing so, it lays down an interesting framework for assessing risk that drives capital requirements. According to Basel II, risk includes the following:

- Market risk—Reflecting the risk from changes in market prices of traded commodities
- Credit risk—Reflecting counterparty risk of nonperformance of financial contracts
- Operational risk—Reflecting the risk from failed internal processes

In addition to these risks, the occurrence of external events is a major source of risk—called exogenous risk—to the modern enterprise. It is important to consider exogenous risk as different from operational risk for two reasons. First, operational risk focuses more on failures of internal business processes, and, second, operational risk is a vast "catch-all" category that does not provide the needed focus on external events that deserve important consideration and management attention. This article differentiates between exogenous and operational risk in that operational risk arises from more inward-looking internal processes rather than external events that are out of the control of the organization, yet can have serious consequences for value. Exogenous risk events include occurrences such as major terrorist acts, the risk of war, the risk to business from pandemics such as SARS and avian flu, disruptive technological events that impact business volumes, changes to the demographic mix of employees or customers, and changes to legislation that reduce the barriers to entry. Some of these events can be predicted in advance, allowing organizations the ability to react in time. Others, by their very nature, cannot be predicted and call for preparation based upon reasonable estimates of risk scenarios.

Based on this, the entire risk universe within which a commercial enterprise operates can be thought of as having four clear components, as shown in **figure 4**.

Figure 4—Four Components of the Risk Universe

Of the four risk types described, market risk and credit risk have been the subject of significant academic study, and there are complex analytical tools available to model and simulate their behavior and risk expectation. There is also an active financial market in credit and financial derivatives where market and credit risks can be transferred to other participants, and corporations can actively measure and manage these risks.

Operational and exogenous risks, however, are what cause the most spectacular value-destroying events and are responsible for the most variability in value. According to the Basel II framework, operational risk that requires a capital allocation comes in the following broad categories:

- Internal fraud
- External fraud
- Employment practices and workplace safety
- Client, products and business practices
- Damage to physical assets
- Business disruption and system failures
- Execution, delivery and process management

The operational risks of the kind described in the Basel II framework apply to all businesses, not merely financial institutions. Operational risk is certainly not easy to measure; in fact, in the simpler approach to managing the required capital for operational risk, the Basel II framework requires putting aside a percentage of gross income arising from operations that are at risk. While this may appear to be arbitrary, it reflects the difficulty in measuring and assessing the impact of operational risk.

Living With Risk

Operational and exogenous risks are probably the most complex risks that managers need to deal with on a daily basis. Every business faces a different set of risks, which makes it difficult to use a standard template to manage risks across organizations or even business lines in the same organization.

Effective risk management is enabled by an organizationwide risk management philosophy that includes a pervasive risk culture requiring managers to think of the risk implications of their decisions. In practical terms, this pervasive risk culture would manifest itself in a number of internal processes, enablers, skills and tools used in the business, including at the very least:

- **A risk identification process**—Identifying what can go wrong with and impede the achievement of organizational or departmental objectives is the first step in risk management. The risk identification process is critical to success because if risks are not understood properly, it will be difficult to do anything about them, and many high-impact risks have a low incremental cost treatment that can be implemented only if a comprehensive risk identification exercise is conducted.

  Available tools for identifying risks include:
  – Analysis of the components of the value chain to determine what must go right
  – Interviews with managers
  – Focus groups
  – Past experience
  – Analyst reports
  – Secondary research using outside research groups

  The risk identification exercise is not merely a listing of what risks the participants in the process perceive (e.g., the number of ways one can slip and fall on the way to work), but needs to be structured in a disciplined way by an experienced risk manager who can help participants identify risk events, their categorization according to a framework, their impact, the breakdown of the causes or triggers to the risk event, the probability, and the accountability for the risk in question.
- **Risk mitigation tools and enablers**—To allow risk management to be a sustained and successful effort, it is necessary to have tools and enablers that allow the organization to organize its efforts, share learning and increase collaboration, including:
  – A risk framework that allows mapping risks to attributes that matter and impact value. The framework may draw upon generic guidelines provided by industry standards such as the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management (ERM) framework, but it needs to be specific to the organization to allow reasonably approximate quantitative expressions of largely qualitative risk measures.
  – A technology-based database of risks, the owners of the risk, the treatment agreed upon, and processes to manage and monitor the risk on an ongoing basis
  – Process workflows that allow monitoring of the environment to proactively identify, assess, analyze, manage and report risks
  – An internal risk web site that allows communication and helps inculcate a risk culture within the organization
  – Clear organizational roles that clarify responsibilities and prevent diffusion of accountability for managing the different types of risk
- **Appropriate risk responses**—Once an organization knows its risks, it is possible to consciously respond to them. Responses to risk may include the following:
  – Acceptance—The organization chooses to live with the risk.
  – Reduction—The organization takes steps to reduce the impact or probability of the risk.
  – Avoidance—The organization chooses to avoid the risk by stepping out of harm's way (e.g., avoiding hurricane risk by relocating away from the coast).
  – Transfer—The organization transfers risk by purchasing insurance (e.g., over-the-counter weather derivatives bought by an energy company to hedge against the risk of low demand).

- **A portfolio approach to risk**—Risks tend to be interrelated in complex ways that should be understood and taken into account when managing them. A portfolio approach to risk using financial portfolio concepts that model the correlation between different risks and their impact should be considered for use. Risks that are positively correlated will tend to magnify their impact, while those that are inversely related will tend to negate each other.
- **Alignment with business strategy**—Risk management needs to be clearly focused on achieving the organization's objectives, of which enhancing shareholder value is paramount. However, enhancement of shareholder value is a generic objective, and its practical implementations generally include goals such as extending market share, increasing billing rates and reducing cost of operations, depending upon the business. Risk management needs to be clearly aligned with business strategy as reflected in the objectives that managers seek to achieve on a day-to-day basis.

The Business Case for Risk Management

Establishing a business case for risk management can be a tricky task, as it is generally not easy to express the benefits from managing risk in pure NPV terms. Trying to establish an NPV (or its other incarnations such as return on investment [ROI] or internal rate of return [IRR]) is not the right approach to justify an investment in risk management initiatives. In fact, it is best if risk management is considered from the risk perspective, i.e., by helping reduce the risk, risk management helps reduce the variability in value added, thereby reducing the return that investors demand from the organization, which in turn creates value by reducing the weighted average cost of capital (WACC) for the business. A reduced WACC increases the capitalization multiple for the business and creates value even without directly increasing cash flows.

For some businesses, risk management is not optional—it is mandated by regulation. The US Securities and Exchange Commission (SEC), for example, has established three business continuity objectives (business continuity planning is an element of operational risk management) that have special importance for all financial firms and the US financial system as a whole. The SEC-established objectives for BCP are:

- Rapid recovery and timely resumption of critical operations following a wide-scale disruption
- Rapid recovery and timely resumption of critical operations following the loss or inaccessibility of staff in at least one major operating location
- A high level of confidence, through ongoing use or robust testing, that critical internal and external continuity arrangements are effective and compatible

Similarly, the requirements of the US Sarbanes-Oxley Act touch upon the need to manage risks relating to financial reporting, an important internal process with significant external implications.

Conclusion

Risk management is not the job of only internal audit, nor that of just the Sarbanes-Oxley project team. It is a part of every manager's job, and the organizational culture should encourage thinking in terms of risk. Managers should evaluate their decisions not merely from an ROI or NPV perspective, but also from a risk-adjusted perspective. A database that formally records the risks facing an organization will also help develop and deploy appropriate risk responses that are aligned with the risk the business's stakeholders are willing to take.

References

Brealey, Richard; Stewart Myers; *Principles of Corporate Finance*, McGraw-Hill, 2005

Bank for International Settlements, *Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework,* 2005*, www.bis.org/publ/bcbs118.pdf*

Copeland, Tom; Tim Koller; Jack Murrin; *Valuation: Measuring and Managing the Value of Companies*, John Wiley & Sons

Endnotes

[1] Enterprise value includes the value of the equity and debt holders of a business. However, since the nominal value of debt remains constant regardless of changes in the riskiness of a company's venture (though the market value of debt may change), for the purposes of this article, changes in enterprise value are considered to accrue entirely to the shareholders. Therefore, all changes to enterprise value are a part of the TRS, the measure of value.

[2] The use of a normal curve as representative of NPV distributions is purely illustrative. Even if the distribution does not follow a normal curve, it does not take away the fact that a higher expected standard deviation would mean a higher risk of a negative outcome.

Mukul Pareek, CISA, ACA, AICWA
is a business consultant based in New York, New York, USA. He has more than 16 years of experience in audit, accounting, finance and IT management. He graduated from the University of Delhi (India) and holds a master's degree from Columbia Business School. He can be reached at *mp@aslpartners.com* or *mpareek@satoriconsulting.com*.

Information Systems Control Journal, formerly the IS Audit & Control Journal, is published by the *Information Systems Audit and Control Association*, Inc.. Membership in the association, a voluntary organization of persons interested in information systems (IS) auditing, control and security, entitles one to receive an annual subscription to the *Information Systems Control Journal*.