Use of the Balanced Scorecard for IT Risk Management

Rajesh Kapur, CISA, FIETE, MIE, is a director at Tyche IT Consultants. He has been a professor of computer science and engineering at BIET, Hyderabad, India; and a faculty member at the Institute of Chartered Financial Analysts of India (ICFAI) Business School, Hyderabad, India. Kapur has been a senior project manager at Synfosys Business Solutions, deputy general manager at the Corporate IT Division of Apollo Hospitals, and director (solutions) at winAMR Systems. He can be contacted at kapursam@rediffmail.com.

Rajesh Kapur, CISA, FIETE, MIE, is a director at Tyche IT Consultants. He has been a professor of computer science and engineering at BIET, Hyderabad, India; and a faculty member at the Institute of Chartered Financial Analysts of India (ICFAI) Business School, Hyderabad, India. Kapur has been a senior project manager at Synfosys Business Solutions, deputy general manager at the Corporate IT Division of Apollo Hospitals, and director (solutions) at winAMR Systems. He can be contacted at kapursam@rediffmail.com.

Risk management, in its essence, is subjective. Though it is a structured approach to determine whether to accept, mitigate, transfer or avoid a risk, it is based on a subjective assessment of the business impact of the exercise on organizational vulnerability. The current slowdown in business profitability has brought into greater focus the need for risk management initiatives to quickly align with the business goals of an enterprise. Business goals will change from time to time, as will the perception of their associated vulnerabilities and their consequent impact. The process of risk management must be in line with this change. In a dynamic business environment necessitating change in business goals and objectives, the “in line” aspect of risk management (with business goals) percolates down to the management of risks associated with the optimal deployment of IT resources.

THE BALANCED SCORECARD

There are numerous factors that impact the business goals and objectives of an enterprise and, thereby, contribute to the need for change. The change may be driven by market forces or may be a result of an internal shift in priorities. These factors, varied and divergent as they are, can be effectively abstracted by means of a balanced scorecard (BSC) approach.

The BSC approach has evolved from its early use as a simple performance measurement framework to a full-fledged strategic planning and management system. It is used across all sectors of business and industry to align enterprises’ business activities to the vision and mission of the organization, to improve internal functioning and customer perception of an organization, and to monitor the organization’s performance against strategic goals. It spawns a framework for performance metrics and delineates objectives, from which management can execute strategies. BSC has the potential to oversee the mechanism of converting a long-term strategic plan into sets of immediately doable activities.

Although a great deal of literature is available on the BSC, it is abstracted for the purposes of this article in figure 1. Each of the four perspectives is briefly elucidated as follows:

- The financial perspective is focused on ensuring that the execution of the strategy of an enterprise is contributing to bottom-line growth. Revenue growth, costs, profit margins, cash flow and net operating income are some illustrative metrics that are incorporated into the planning and evaluation of an enterprise’s activities vis-a-vis this perspective.

- The customer perspective is focused on the value proposition (based on the appropriate mix of operational excellence, customer relationship management and product share) that the enterprise implements to generate greater sales by courting its customers.

- The internal business processes perspective focuses on the processes that create and deliver the product’s value proposition for the customer. Included in these processes are those that deal with (but are not limited by) operations, regulation, compliance, innovation, and the discharge of social and corporate responsibility.

- The learning and growth perspective focuses on the foundation of any strategy: the intangible assets of an organization, which primarily comprise the internal skills and capabilities that are required to mentor and support the value-creating internal processes. Though investment in these assets usually decreases the short-term bottom line, it is necessary to realize long-term goals and success of an enterprise.

Do you have something to say about this article? Visit the Journal pages of the ISACA web site (www.isaca.org/journal), find the article, and choose the Comments tab to share your thoughts.
The BSC methodology can provide a measurement and management system that supports the process of IT governance as well as the more critical aspect of alignment of IT governance to corporate goals and objectives. Under this proposal, an IT BSC links with business through the business contribution perspective—by explicitly expressing the relationship between IT and business via a mapping of business goals and objectives to IT goals and objectives. The IT BSC, after mapping the various perspectives, is shown in figure 2 (the mapped IT perspectives are shown in bold italics).

The mapping is a tool used to provide direction on how to impart maximum value for the organization through technology. It traces the consequential relationship between strategic goals determined by the corporate BSC and the consequent strategic objectives as relevant to the IT domain of an IT BSC (the respective objectives are within ovals in figure 2). For example, improving performance in the objectives found in future orientation (learning and growth) enables the organization to improve its operational excellence (internal business processes), which in turn enables the organization to create desirable results in the customer and financial perspectives. There is a cause-and-effect relationship here that plays out as the enterprise moves through various stages of its life cycle.

IT departments can control risk by developing and deploying application controls to ensure completeness, accuracy, validity, authorization and segregation of duties, but accruing business value through risk management will require an understanding of the current priorities of the enterprise—in effect, those of senior management. These would be guided not only by various social, economic and environmental factors, but also by the specific stage of the life cycle of the enterprise.

Risk management, subjective as it may be, has to be an inherent aspect of any successful business effort; it is carried out either explicitly or implicitly at both the operational and strategic levels of an enterprise. It is an essential constituent of sound corporate governance. Just as the IT BSC can be deduced from the corporate BSC to better align itself with corporate business objectives, a methodology for technology risk management can be deduced from the corporate BSC to facilitate effective IT risk management.

This article aims at extrapolating the technique of using the BSC for IT governance to the task of IT risk management for an enterprise. It factors in the cause-and-effect relationship elucidated previously. Deployment of the methodology will enhance the level of sensitization of the technology risk management process to its most critical requirement—alignment with corporate goals and objectives.

The Methodology

The methodology includes the following seven steps (see figure 3):

- **Step 1**: Identify the current set of BSC goals. This activity is carried out at the highest levels of the organization. The chief information officer (CIO) must keep abreast of the goals and must ensure that any noticeable shift in priorities is (implicitly or explicitly) detected and expeditiously translated into an IT risk management plan.
Step 2: Map the current set of BSC goals to actionable technology objectives, and establish the context in which the risk assessment framework is applied to ensure appropriate outcomes. This should include the objective of the assessment to a BSC goal, including delineating the context of each risk assessment against the business criteria sought to be achieved.

Step 3: Develop a risk identification system based mainly on the objectives determined in step 2. The main activities to be carried out at this stage are the profiling of specific threats and vulnerabilities to the attainment of the objectives.

Step 4: Carry out a risk assessment, taking into account the probability of occurrence, business impact (of the occurrence of vulnerability) and prioritization as per the standard methodology. Information security and compliance are not the only issues here. Threats to competitive advantage, reputation, furthering the mission, etc., have to be considered. Only by a holistic consideration of the entire spectrum of an organization’s activities and due prioritization is a technology risk assessment finalized.

Step 5: Determine the specific risk control strategy as a combination of one or more of the following, in respect of each risk assessed:
- Risk avoidance
- Risk transfer
- Risk mitigation
- Risk acceptance

Step 6: Implement the system as per the system development life cycle (SDLC) methodology, with the enumerated strategy as an integral part of the requirement and analysis phases. This is the stage at which a risk response process should be developed and maintained. It should be designed to ensure that cost-effective controls align themselves with the specific risk control strategy chosen on a continual basis. Provisions for making allowance for risk management due to compliance and regulatory guidelines would be in addition to the risk management efforts deduced from the BSC.

Step 7: Periodically review whether the technique is proving effective. The associated metrics will have to be identified at the initial stages. The final assessment must also be modulated by the subjectivity inherent in all risk-related activities. Some suggested metrics are:
- The percentage of risk management effort that is earmarked, as a result of BSC priorities, as a part of the overall risk management effort. It is suggested that this should not be less than 60 percent.
- The percentage of actual critical events that have impacted business as a part of those envisaged during the risk assessment stage
- Number of significant incidents caused by risks not identified in the risk management process, as well as their respective business impact
- Frequency of review of the technology risk management process
- Cost-benefit analysis of the implementation of the controls

Figure 3—IT Governance BSC Methodology

CRITICAL SUCCESS FACTORS
Risk management has now become inherent in all corporate endeavors. Getting all the stakeholders to focus on true essentials remains a challenge. Critical success factors (CSFs) help in delineating the essential areas of activity that must be performed well to achieve business goals.

The CSFs for technology risk management through the use of the BSC are as follows:
- The priorities as set by the BSC must be unambiguous and based on technology abstractions by the CIO (function) that have been mapped from facts sourced from:
  - Business intelligence and data
  - Stakeholder expectations
- The mapping from technology abstractions to discrete IT objectives must be parameterized, and thresholds must be set for each parameter. In the absence of past data, approximation and estimation techniques should be employed.
- The risk assessment must always make allowances for performance, scale, security and disaster, apart from the objectives set by the BSC.
• Change management must be effective whenever there is a shift in corporate priorities. This includes:
  – Identifying the drivers of the change and their respective responsibilities (i.e., who will do what)
  – Establishing a road map for change along with the milestones
  – Ensuring that monitoring and controls are in place on a periodic basis

CONCLUSION
At the end of the risk management activity, there is always a question that the stakeholders would like to have answered with a fair amount of certainty: “Have we got it right?”

The question can be answered to any acceptable amount of precision only by constant observation and review—by being proactive rather than reactive.

Success in any technology risk management activity, however, relies heavily on the commitment shown by senior management; the competence of the risk assessment team to translate business requirements into IT objectives; the support and participation of the IT team; and the awareness, cooperation and support of all employees in the organization who must comply with the controls to make the vision of their organization a reality.

REFERENCES
Fischer, Urs; “Identify, Govern and Manage IT Risk
Part 1: Risk IT Based on COBIT Objectives and Principles,”
ISACA Journal, vol. 4, 2009

Schlarman, Steve; “IT Risk Exploration: The IT Risk
Management Taxonomy and Evolution,” ISACA Journal,
vol. 3, 2009

Nash, Kim S.; “Armed for Safety,” Real CIO World,
vol. 4, issue 5, 15 January 2009


Buchler, Kevin; Andrew Freeman; Ron Hulme; “The New
Arsenal of Risk Management,” Harvard Business Review
South Asia, September 2008

Stoneberner G.; et al; “Risk Management Guide for
Information Technology Systems,” Special Publication,
800-30, National Institute of Standards and Technology
(NIST), July 2002

ENDNOTES
1 Van Grembergen, W.; “The Balanced Scorecard and
IT Governance,” Information Systems Control Journal,
vol. 2, 2000

EDITOR’S NOTE
Collaborate with ISACA members and access additional resources on this topic in the ISACA Knowledge Center located at www.isaca.org/knowledgecenter.