SOCIETY OF ACTUARIES

Article from:

Risk Management

July 2005 – Issue 5

Operational Risk Assessment in IT Projects

by Michel Rochette

Operational risk can sometimes be a broad and elusive concept. A definition is thus necessary. The accepted definition within the financial community is to define operational risk as the risk of direct and indirect losses resulting from inadequate or failed internal processes, systems, people or external events. This is also the definition that is used by the majority of financial institutions that estimate the amount of economic capital required to cover this unexpected consequence of this risk, as mandated by some new regulatory standards.

However, for internal purposes, institutions may want to add other risks to the definition of operational risk in order to satisfy additional business goals. For example, some institutions want to assess the qualitative or quantitative impacts resulting from events affecting their reputation. Others are measuring strategic impacts as well. Others are becoming interested in assessing risks that pertain to projects.

These projects can be new products, new geographic locations, new ventures, overhaul of existing operations, new IT software development, etc. They involve many people, many steps, many processes, many systems and are affected by external events. Thus, assessing and managing the many risks faced by any project will help an organization reduce the likelihood of its failure and contribute to a better use of its limited human and monetary resources to the management of the most risky ones.

A possible approach to assess the riskiness of a project is the scorecard approach in risk management. It has a lot of similarities to traditional actuarial and underwriting of risk. The first

Table 1

Operational Risk Category	Risk Drivers
IT Systems	• Number of providers • Level of technological reliability • Technical complexity • Number of links to existing and future systems
Process and Human (Direct Implementation)	• Number of providers • Relative size of the project • Team diversity • Length of project • Definition of roles • Number of steps in the project • Team expertise
Process and Human (Indirect use)	• Number of changes to the processes • Expertise of the uses of the IT systems • Number of internal and external users
Credit	• Financial capacity of the IT providers
Legal	• Number of legal contracts to negotiate
External	• External events outside the organization

Michel Rochette, FSA, MAAA, MBA, is an actuary specializing in risk management for CDP Capital in Montreal, Quebec. He can be reached at *mrochette@lacaisse.com.*

component is the identification of operational risk drivers or risk factors that might cause a project to fail (see Table 1 on page 38). In other words, the determination of the factors that explain the frequency of failure of the project. These risk drivers are then rated. A similar approach is done for the likely impacts following failure—monetary or non-monetary—taking into account the effectiveness of controls that are put in place to mitigate its failure. Then, the riskiness of the project—the project risk score—is measured as the rated frequency times the rated impacts net of controls. Then, depending on the risk tolerance of the organization, a decision is made to go ahead or not with the project and necessary resources are allocated to manage its resulting risks.

The rest of this article briefly explains such an approach. It was developed for the assessment of operational risk for IT projects. It has now become an integral part of the process to make decisions about IT projects in my company. In fact, standards like COBIT in IT software development usually mandate this analysis.

The first component of the project risk score is the calculation of the score for the frequency. It is obtained by scoring the risk drivers that explain incidents from the IT systems themselves—from direct processes related to the implementation of the IT systems, indirect processes related to the use of the new IT systems, human fraud, legal incidents resulting from negotiating IT contracts, the credit failure of the companies providing the IT systems and other external events affecting the project overall.

Table 1 on page 38 lists the main risk drivers for each category of operational risk for the IT project. They were chosen because of the fact that they can be measured easily from the information that is usually part of an IT project like the forecasted budget, the time associated with it, the number of people involved, etc. Also, they were cross referenced to the many published articles on the subject over the years.

Each risk driver was scored as a null, weak, moderate or high risk (see Table 2). Then, a number was assigned for calculation purposes. The risk scoring reflects knowledge of the IT experts and the risk tolerance of the organization, as well as taking into account the size and scale of the organization. Over time, these scores will be translated in probabilities as experience is accumulated.

For example, the score associated with the number of providers was determined based on the following scale.

Table 2: Example of the Risk Scale of a Risk Driver Number of Providers

Risk Driver	Score
No provider	Null (0)
1 provider	Weak (1)
2 to 3 providers	Moderate (2)
More than 3 providers	High (3)

Once all risk drivers were scored, the overall riskiness for the frequency was calculated simply by averaging all risk scores. It would also be possible to weigh more some risk drivers, and the average score could be further analyzed separately for each risk category.

The second component of the project risk score is the calculation of the score for the monetary impacts from potential incidents in each risk category (see Table 3 on page 40).

Again, a similar approach to the frequency component was followed. The impact for each component of risk was estimated as a percentage of the relevant IT budgets.

To determine the overall riskiness related to the impacts of the project and to add some conservatism, all monetary impacts were simply summed. We didn't take into account non-monetary impact for the time being. Then, reflecting past expert knowledge and the risk tolerance of the organization, the overall impact of the IT project was scored on a scale of null, weak, moderate and high risk (see Table 4 on page 40).

continued on page 40 ◗

Risk Management
Issue Number 5 • July 2005

Published by the Society of Actuaries
475 N. Martingale Road, Suite 600
Schaumburg, IL 60173-2226
phone: (847) 706-3500
fax: (847) 706-3599
www.soa.org

This newsletter is free to section members. A subscription is $15.00 for nonmembers. Current-year issues are available from the Communications Department. Back issues of section newsletters have been placed in the SOA library and on the SOA Web site: (www.soa.org). Photocopies of back issues may be requested for a nominal fee.

Operational Risk Assessment in IT Project

◗ continued from page 39

Table 3

Operational Risk Category	Monetary Impacts
IT systems	Budget for the IT equipment and software
Process and Human (Direct implementation)	Budget for the internal and external human employees and consultants
Process and Human (Indirect use)	50% of the total IT budget
Credit	50% of the the budget of the IT providers
Legal	1% of the total IT budget
External	1% of the total IT budget

Table 4: Risk Scale for the Monetary Impact

Total Monetary Impacts (Exposure)	Score
Less than $50,000	Null (0)
Between $50,000 and $100,000	Weak (1)
Between $100,000 and $250,000	Moderate (2)
More than $250,000	High (3)

Table 5: Risk Scale for the IT Project Risk Score

IT Project Risk Score	Score
0	Null
Between 1 and 3	Weak
Between 4 and 7	Moderate
More than 7	High

And as actuaries are familiar, an overall risk score is calculated as the product of the frequency and impact score. Then, for internal communication purposes, instead of talking in terms of expected averages, the IT project risk score has been communicated as words using the following scale (see Table 5).

So far, 14 IT projects in 2005 have been analyzed using this new approach. More than one third of the IT projects had a risk score that ranked above moderate. Given these risk scores, more resources in project management were allocated to these respective projects, resulting in a better allocation of the firm's resources and, indirectly, economic capital.

Some refinements are under way, like integrating the effectiveness of controls—control score—in this process. This is particularly relevant given the interest firms have in certifying their financial statements under the new SOX regulatory standard. Also, it is envisioned that a more refined risk assessment will be developed as loss data is accumulated, which will allow us to be able to statistically measure some of these components.

Finally, this has been an interesting project to demonstrate to different groups in my company how my actuarial background, along with the knowledge developed over the years in the field of risk management, could help it better assess and manage the operational risk resulting from IT projects. ✦