Gartner

Research

Publication Date: 23 June 2004 **ID Number: G00121489**

CIO Update: How to Assess and Mitigate IT Project Risk

Matt Light, Jack Heine

With proper assessment and risk management, launching complex IT projects can be strategically sound. However, when risks are badly assessed or untracked, and no mitigation plans exist, the result can be hazardous to a project's health.

ANALYSIS

Missing the Danger Signals

Project sponsors' business cases typically draw attention to the benefits of their proposed projects, but cost/benefit analyses seldom attempt to identify the risks that a project could pose to the overall portfolio. Danger signals involving risky projects often go undetected well into a project's life, even as resource and duration requirements become clear.

As a result, IS organizations typically expend substantial resources on projects that are eventually canceled. You can avert this wasted effort with proper risk assessment and management. By this, we don't mean merely managing schedule risk (for example, via a Monte Carlo-style simulation to anticipate critical path schedule slippage), but assessing both project and portfolio risk.

Any tardy or canceled project in the portfolio is comparable to a delay on the critical path of a project: A late project draining vital resources can throw off several other projects' plans. Therefore, prior to chartering a project, you should make a disciplined risk assessment of any project likely to take more than a few person-months, using the process we'll describe in this research.

A Formalized Risk Assessment Methodology

In their book, "Megaprojects and Risk: An Anatomy of Ambition," Flyvbjerg, Bruzelius and Rothengatter debunk the "EGAP principle" — Everything Goes According to Plan. According to Flyvberg et al., "The most consequential problem regarding risk analysis ... is not the absence or inadequacy of risk analysis in itself, but the neglect of relevant downside probabilities in the calculation of project viability." "A technique that should be made use of in feasibility studies ... is the analysis of worst case scenarios," they conclude, and Gartner agrees.

A formalized risk assessment methodology is beneficial from several perspectives. First, using a formula to assess risk forces the consideration of items that might normally be overlooked. Second, a formal risk assessment process ensures that you can view several projects from the vantage point of uniform risk.

Gartner's Guidelines

The first step in formalizing IT project risk is to start with a definition. The method of risk assessment Gartner recommends uses the following guidelines.

- *Risk Index*: Sum of weighted vulnerabilities times the probability of occurrence/number of vulnerable items.
- *Risk Index:* The comparative value of associated risk, with the highest value equating to the highest risk, in which a value of 1.0 indicates a certainty.
- *Vulnerabilities:* The areas in which the project is weak or susceptible to failure.
- *Weighted Vulnerability:* A value, ranging from 1.0 to 5.0, that is assigned to the vulnerable area based on its degree of impact on the project.
- *Probability of Occurrence:* The statistical likelihood that the project will experience one or more vulnerable events.

To use this formula-driven approach for assessing project risk, you should first identify the areas of vulnerability for each project. Your goals and specific requirements should be detailed, so that

you can rate the project from low risk to high risk, that is, from 1.0 to 5.0, respectively, in the areas of vulnerability, rather than overall.

For example, the six areas that typically threaten an IT project are technology, schedule, complexity, operational, business and organizational (see the sidebar, “Six Aspects of IT Project Risk”). In addition, larger projects clearly involve greater time and expense, so they pose a greater risk. Therefore, you should make project size estimates for the business case using systematic estimating techniques. For example, a “large” rating of 5.0 might be for a project estimated at more than 30,000 staff hours.

Potential of Project Vulnerability

Items that may indicate a potential of project vulnerability include “yes” answers to the following:

- Will multiple physical installations extend project implementation?
- How much will the project schedule depend on the availability of end-user staff for analysis and testing?
- Is the end date fixed or flexible?
- Are there several complex deliverables?
- Will the project change entire business processes?
- How severely will user procedures change under the proposed system?
- How large is the user population? How diverse is it?
- Are the functional requirements clear or vague?
- Will the system depend on many other business systems?
- Will the new system require new maintenance procedures?
- Will the proposed system adhere to enterprise standards?
- Are more than three distinct systems involved?
- Are critical tasks out of the project team’s control?
- Will the project require major hardware or software upgrades?
- Must multiple departments provide resources to the project?
- Will the IS staff be continuously available throughout the project?
- Is any software (such as language, database, communications or tools) for the project new to the development team?
- Is any hardware new to the development team?
- Will construction require complex and intricate logic?

If you answer “yes” to any of the above questions, you should assign an impact value — on a 1.0-to-5.0 scale (1.0 being minimal, 5.0 being substantial). This step begins to indicate the potential impact of the vulnerability associated with the project.

Probability of Occurrence

Next, you should assign a probability of occurrence for each item of vulnerability. Consider using a value within a range estimate, such as 0.1 to 0.3 equals unlikely, 0.4 to 0.6 equals somewhat likely and 0.7 to 0.9 equals very likely (see Figure 8).

Figure 8. IT Project Risk Assessment

Vulnerabilities	Weight	Probability	Weighted Probability
Complex Deliverables	3	0.3	0.9
Severe Changes to User	2	0.5	1.0
System Interdependence on Other Systems	5	0.7	3.5
Sum of Weights	10		5.4
Divide the weighted probability by the sum of the weights to derive the risk index: 5.4/10 = 0.54, which indicates a moderate risk associated with this project effort.			

Source: Gartner Research (June 2004)

Consider these items in assigning a probability:

- How much control does the project have over this outcome?
- Has IS/application development staff experienced problems in this area previously?
- Do you expect any problems in this area?

At this point, you will have a list of vulnerabilities and a probability of occurrence for each project. Your next step is to determine a weighted average of the total vulnerability by multiplying the vulnerability factor (1.0 to 5.0) by the probability of occurrence. You then divide this result by the sum of the vulnerability factors. Following this step, you can stack rank the project list by probability of failure.

Assess a Monetary Risk

Your final step is to assess a monetary risk associated with the project, and to multiply this value by the probability of failure for the entire project. The result is a monetary value for the risk associated with the project.

Consider the following when estimating the magnitude of potential loss:

- What is the estimated cost of the entire project?
- Will business success depend on the project, and, if so, what is the potential impact, as estimated by the business?
- Could implementation interrupt mission-critical operations and what would be the financial impact of such interruptions?

Mitigating the Risks

After you've determined a monetary risk value for each item of vulnerability, you can conduct a review of opportunities to mitigate the risks. You may have opportunities to significantly reduce risks through changes in project scope, timing, resource allocation and so forth. Through this exercise, you may move some projects from being considered high risk to moderate or low risk.

Through 2008, IS organizations without stringent risk-assessment procedures and mitigation plans will cancel at least 10 percent of projects initially budgeted at more than $200,000 and at least 20 percent of all projects (0.7 probability).

Gartner provides a sample list of risk management tools (see the sidebar, “Representative Risk Management Tools”).

Bottom Line

- You should perform this risk-assessment exercise for each project in the portfolio as a way to determine which projects represent high-risk endeavors.
- The analysis of feedback gathered during the risk-assessment process may also offer an indication of common weaknesses within the organization.
- For example, if many projects suffer from the same risk areas, then you should probably address this issue from an organizational perspective, rather than a project view.

Six Aspects of IT Project Risk

- *Technology Risk:* Chosen technologies, especially if new or “cutting edge,” may have performance, reliability or security issues, or they may be subject to skills shortages.
- *Schedule Risk:* The probability that the project can be implemented within expected schedule.
- *Complexity Risk:* The risk of failure due to magnitude of the complexity involved, because of its scale, the degree of change required or the number of parties involved.
- *Operational Risk:* The degree of certainty of estimated total cost of ownership or ongoing operating costs.
- *Business Risk:* Changes to economic or other conditions may negatively affect the business case.
- *Organizational Risk:* Internal changes may prevent the completion of a project or the realization of returns.

Representative Risk Management Tools

C/S Solutions

Risk+ for MS Project —

www.cs-solutions.com

Palisade

@RISK — www.palisade.com

Pertmaster

Risk Expert — www.pertmaster.com

Monte Carlo for Primavera

Primavera — www.primavera.com

RiskTrak

Risk Services and Technology —

www. risktrak.com

RMC Project Management

Various risk assessment and management training tools — www.rmcproject.com

SmartOrg

Portfolio Navigator and Decision Advisor — www.smartorg.com

Welcom Software Technology

WelcomRisk — www.wst.com

Written by Edward Younker, Research Products

Analytical sources: Matt Light and Jack Heine, Gartner Research

This research is part of a set of related research pieces. See "Inside Gartner Top View" for an overview.

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Level 7, 40 Miller Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Latin America Headquarters
Av. das Nações Unidas 12.551
9 andar—WTC
04578-903 São Paulo SP
BRAZIL
+55 11 3443 1509

Gartner