SUBJECT

INFORMATION SYSTEMS PROJECT MANAGEMENT

TOPIC: Session 8:Risk Management in IT Projects – case study

sasanana1
[Pick the date]

Session 8:Risk Management in IT Projects – case study

Case study about : Markus Gaulke, CISA

The risks associated with electronic data processing represent a majority of today's companies' operational risk. In addition to the mere operating risk, the successful completion of complex IT projects has a major strategic impact on enterprises and their competitiveness. The operational risks resulting from IT projects can be reduced substantially through efficient risk management. IT auditors therefore must be involved more actively in project risk management.

Since 1 May 1998, public limited companies in Germany are obliged by law (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich) to implement a monitoring system that enables them to perceive in advance developments that could jeopardize the continuity of the company. Thereby, for the first time, German legislators explicitly requested all enterprises systematically to record all business risks and to manage the identified threats.

With the increasing dependence on IT and exposure of companies to electronic data processing, the technological risks (as part of operational risks) are becoming more significant in the business environment. Therefore, technology (i.e., hardware, software, system security) also is one of four major categories a working group in Germany has developed as a proposal for the classification of operational risks in the context of the Basel II consulting phase. The suggested categorization of operational risks also includes an operational risk category, "Processes and Project Management." This risk category has played a minor role in many companies, although the execution of project tasks always has been associated with a substantial business risk.1

Basel II and Operational Risk

On 16 January 2001, the Basel Committee on Banking Supervision announced a second consulting paper for the New Basel Capital Accord (Basel II). The new regulation about equity capital, which most certainly will become effective in 2005, also comprises approaches to measure operational risks. In the Basel papers operational risk is defined as "the risk of losses resulting from inadequate or failed internal processes, people and systems or from external circumstances."2 The reason for the inclusion of operational risks in the New Basel Capital Accord is the increasing importance of these risks. A survey conducted by the Bank of England examining the main causes of problems within banks

showed inadequate systems and controls at the first place.3Especially, complex IT projects have inherent operational risks, either during the projects themselves (e.g., because of insufficient allocation of resources) or after the projects end (e.g., because of insufficient system design).

It has been reported that US companies are investing US $250 billion in IT projects each year.4 The technological change and the increasing competition are requiring permanent changes to existing IT and communication systems. Obviously, a successful company must be able to carry out projects in a professional way to launch new high-quality products and services in time.

The necessity to consider risk management in IT projects is evident from the results of numerous surveys,5 which show a high number of projects that missed their targets or that came up with a substantial overrun in time or budget. A survey by KPMG6 on failed IT projects showed that 45 percent of the observed IT projects could not realize the expected benefit. In addition, 87 percent of the observed IT projects exceeded the projected time frame, and 56 percent exceeded the planned budget by more than 30 percent. With the implementation of a professional risk management, the occurrence of project failures effectively can be avoided.7

Risk Management Process for IT Projects

To identify the risks of an IT project in good time, a systematic project risk management should be implemented with the inauguration of the project. (See **figure 1**.) The risk management process at project level can be divided into the following phases:

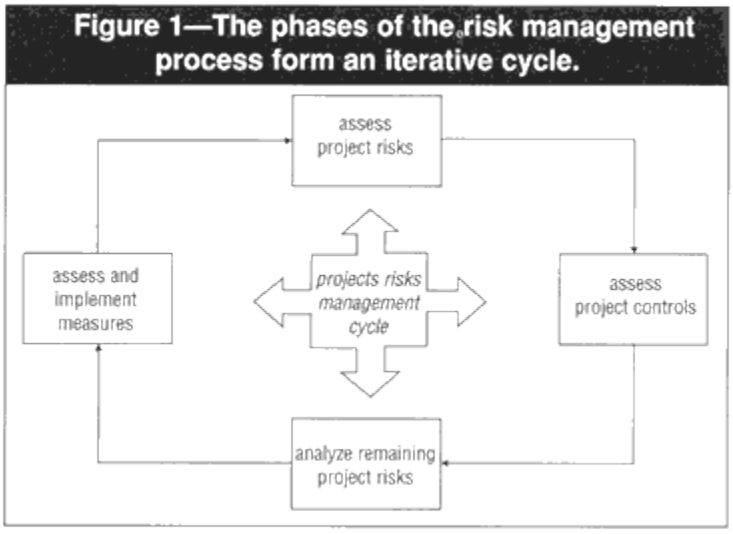


Figure 1—The phases of the risk management process form an iterative cycle.

- Assessment of project risks
- Assessment of project controls
- Analysis of the remaining project risks
- Assessment and implementation of measures
- Permanent monitoring of project risks, controls and measures

Assessment of Project Risks

The crucial factor for an efficient risk management in IT projects is the systematic identification of the inherent project risks and the assessment of the existing project controls. Project risks are potential threats to the success of the project. Inherent risks are threats that exist fundamentally within a process, i.e., before controls are implemented. These inherent risks depend on--among other things--the type of project, the business area and the technology used. The systematic identification of inherent project risks should be based on a comprehensive risk catalogue, summarizing the experiences of many projects.8 For such a risk catalogue, a categorization in the following six major project areas is recommended:

- Project management
- Business focus
- Business processes
- Users
- Technology
- Data

For such a risk checklist to be consistently applicable, project management should determine critical key questions for each project area and to explain each key question with more questions and examples. In the risk checklist provided here, a key question in the technology project area for the inherent project risk "New Technology" is "Does the success of the project depend on technologies that are novel and with which the company has little or no experience?"9 In addition, a rating scale for the inherent risks is provided for each key question. The aim of this analysis is to determine the inherent risks for each project area, which is then evaluated in more detail in the following phase. (See **figure 2**.)

Assessment of Project Controls

To evaluate the project risks, the project controls in the defined major project areas must be identified and assessed for their effectiveness. The identification and evaluation of these project controls must be as systematic as the identification of the project risks. To evaluate the project control procedures in each project area, control questionnaires and best practice examples are used. The software development procedure in the technology project area, for example, is a project control that is assessed by the key control question: "Does the software development follow a standardized procedure model?"10 For each control question, further explanations and references to typical audit proofs (e.g., documentation of typical software development procedures) facilitate a consistent assessment of the effectiveness of the project controls.

Risk Management in IT Projects

Reduces IT Costs

In times of reduced IT budgets, project costs are considered to be one of the major areas where IT expenditures can be noticeably reduced. According to a survey by McKinsey, project costs constitute about 40 percent of the IT budget. For a long lasting reduction of project costs, a framework for an efficient project management has to be developed.11 Risk management in IT projects consists of a small initial investment that can be expected to pay for itself quickly. The early identification of project risks and the timely taking of project control measures leads to a reduction of overall project costs.12 Project risk management has even more advantages with project failures, for every day earlier a big project is terminated (e.g., because of a systematic project risk management), the company easily can save thousands of dollars (US)--even taking into account a substantial amount of fixed costs.

Analysis of the Remaining Project Risks

Weighing the evaluated inherent risks against the existing controls, it is possible to determine the remaining project risk for each critical project area as well as for each project threat. Such a scalable risk assessment allows a very focused definition and implementation of measures in the subsequent phase.

Assessment and Implementation of Measures

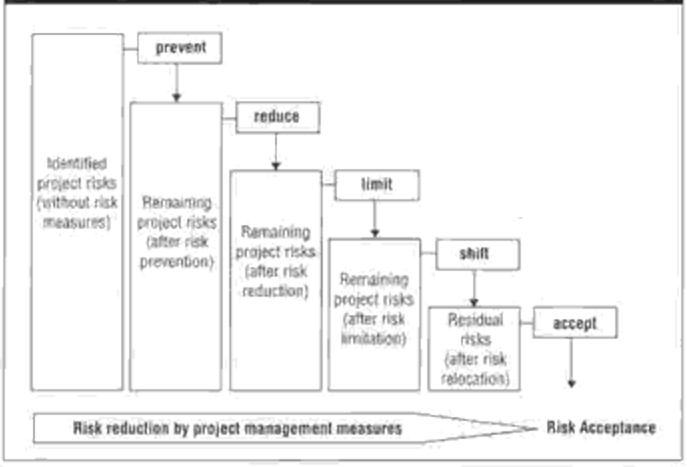
In this stage of the project risk management process, measures for a further risk minimization can be defined on the basis of the analyzed project risks. The weighting of risk factors as the product of a measure (e.g., one equals very small; up to 5 equals very high) of the probability of occurrence and the impact/level of damage that would result from occurrence can be helpful for prioritizing the measures designed to reduce risk. These risk factors ought to be determined on the basis of the risk analysis carried out and the discussions with the responsible project managers and stakeholders.

A helpful tool for determining the appropriate measures is a risk reduction staircase13 which includes the following types of measures:

- Risk prevention (e.g., by change of the project scope)
- Risk minimization (e.g., by remedying the identified poor project controls)
- Risk limitation (e.g., by developing alternatives in case of a project failure)
- Risk relocation (e.g., by agreeing on contractual damages)
- Risk acceptance

The defined measures have to be integrated in the project plan and should be monitored by the risk manager. In addition, management should identify a risk owner for each project risk that is responsible for the realization of the specific measures and thereby, for the management of this risk. (See **figure 3**.)

Figure 3—The risk reduction staircase offers support for the determination of measures.



Permanent Monitoring Project Risks, Controls and Measures

A one-time risk assessment for an IT project is not sufficient for achieving comprehensive risk management. In fact, the evaluation of the project risks and controls should be repeated over the whole project life cycle, and further measures should be defined and implemented, if necessary. In this context, risk indicators as well as control indicators, which represent an objective measure for changes to the risk and control situation, are helpful instruments for defining and monitoring risk and control levels. In the technology project area, the complexity of an IT project could be monitored by the risk indicator "number of interfaces."[14] An example for a control indicator monitoring the effectiveness of the configuration management process could be the "number of modules checked out for longer than x days." For further hints on indicators, readers also can refer to the COBIT *Management Guidelines*.[15] Experience has demonstrated that risk management should not be the responsibility of the project manager. In fact, an independent unit should regularly monitor the state of the project risks and controls to avoid a routine blindness. An IT auditor with project experience and knowledge of project risk management would be an ideal project risk manager.

Conclusion

The successful management of projects has gained a strategic significance for the competitiveness of companies. Nowadays, information technology is an essential part of most projects; even traditional business branches cannot survive without electronic data processing. Therefore, the risks connected with the realization of IT projects constitute a substantial part of the operational risks within an enterprise.

In the next decade, project risk management will be one of the central topics within the management and organization of IT projects. The legislature and supervisory authorities have realized the importance of managing project risks and IT risks in the context of operational risks and, therefore, already have

provided some general framework for enterprises. The further improvement of existing legislative and regulatory frameworks for the management of operational risks can be expected. The IS control and audit profession must be aware of these important developments.

Markus Gaulke, CISA
is senior manager with KPMG Information Risk Management (IRM) in Frankfurt, Germany. He specializes in project risk-related work within the banking and finance sector. He recently published a book on risk management in IT projects, Risikomanagement in IT-Projekten, and he will be the editor of a handbook on Basel II in 2003. For further information, contact him at MarkusGaulke@kpmg.comor www.markus-gaulke.de.