Risikomanagement in IT-Projekten

Vorschlag einer Vorgehensweise

Markus Gaulke

KPMG Deutsche Treuhand-Gesellschaft AG, Frankfurt
(markusgaulke@kpmg.com)

Abstract: The paper outlines the necessity for risk management in IT projects and describes a risk management process and methodology to identify the risks of an IT project in advance. The methodology has been developed 1999 within KPMG, and applied in many firms all over the world. In 2002 the risk management process and the methodology was revised and afterwards published by the author.

1 Notwendigkeit von Risikomanagement in IT-Projekten

Die mit der elektronischen Datenverarbeitung verbundenen Risiken stellen einen bedeutenden Anteil des operativen Risikos einer Unternehmung dar. Der technologische Wandel und der zunehmende Wettbewerb erfordern, permanent Änderungen an den bestehenden IT- und Kommunikationssystemen vorzunehmen. Allein U.S.-Unternehmen investieren jedes Jahr 250 Milliarden Dollar in IT-Projekte [Jo99]. Die erfolgreiche Bewältigung komplexer IT-Projekte hat für die Wettbewerbsfähigkeit von Unternehmen erhebliche strategische Bedeutung. Ein erfolgreiches Unternehmen muß in der Lage sein, Projekte professionell durchzuführen, um neue Produkte und Dienstleistungen in hoher Qualität zeitgerecht einzuführen.

Die Notwendigkeit eines Risikomanagement in IT-Projekten ergibt sich vor allem aus der (auch durch verschiedene Studien belegten [Jo99,WSJ00]) hohen Anzahl von Projekten, die ihr Projektziel nicht erreichen oder erhebliche Zeit- und Budgetüberschreitungen aufweisen. Durch die Einführung eines professionellen Risikomanagements kann solchen Fehlentwicklungen rechtzeitig gegengesteuert werden. Risikomanagement ist daher auch Bestandteil aller wichtigen internationalen Standards für Software-Entwicklung (u.a. CMM [HS87], BOOTSTRAP, SPICE [St99]) oder Projektmanagement (u.a. Guide to the Project Management Body of Knowledge [PMI00]).

Von der gesetzgeberischen Seite sind Aktiengesellschaften in Deutschland seit dem 1. Mai 1998 durch das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) zusätzlich aufgefordert, ein Überwachungssystem einzurichten, um „den Fortbestand der Gesellschaft gefährdende Entwicklungen“ frühzeitig zu erkennen (§ 91 Abs. 2 AktG). Damit hat der deutsche Gesetzgeber Unternehmen erstmals explizit aufgefordert, alle Unternehmensrisiken systematisch zu erfassen und erkannte Bedrohungen zu bewältigen. Neben Geschäftsrisiken (u.a. Produkt- und Haftpflichtrisiken), Finanzrisiken

(u.a. Kredit-, Zins- Währungsrisiken) sowie sonstigen Risiken (wie Umweltrisiken) sind dies im wesentlichen operative Risiken.

Durch die zunehmende Abhängigkeit der Unternehmen von der elektronischen Datenverarbeitung nehmen die technologischen Risiken unter den operativen Risiken eine exponierte Stellung ein. Technologie (u.a. Hardware, Software, Systemsicherheit, Haustechnik) ist dementsprechend auch eine von vier Kategorien, die eine Arbeitsgruppe beim Bundesverband Öffentlicher Banken Deutschlands e. V. (VÖB) als eigenen Vorschlag für die Kategorisierung operationaler Risiken im Rahmen der Konsultationsphase für Basel II erarbeitet hat. Die Vereinbarung "Basel II" des Basler Ausschusses für Bankenaufsicht hat am 16. Januar 2001 ein zweites Konsultationspapier zur neuen Basler Eigenkapitalvereinbarung (Basel II) veröffentlicht. Die neuen Regelungen enthalten insbesondere eine Reihe von einfachen und fortgeschrittenen Ansätzen zur Messung des Kreditrisikos und des operationellen Risikos. Die endgültige Fassung der neuen Eigenkapitalvereinbarung soll Anfang 2003 veröffentlicht und in 2006 umgesetzt werden [Ga02c].

Die vorgeschlagene Kategorisierung operationaler Risiken enthält mit der Kategorie „Prozesse und Projektmanagement“ aber auch ein operatives Risiko, das in der Unternehmenspraxis bisher häufig nur eine untergeordnete Bedeutung hatte.

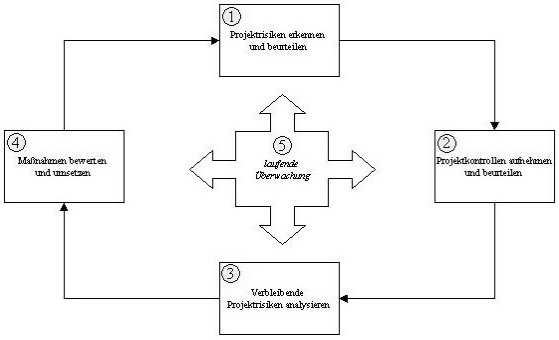
2 Risikomanagement-Prozeß für IT-Projekte

Um die Risiken eines IT-Projektes frühzeitig zu erkennen, sollte schon bei Projekt-Initiierung ein systematisches Projektrisikomanagement eingerichtet werden. Der Prozeß des Risikomanagements auf Projektebene kann dabei in folgende Phasen gegliedert werden:

1. Erkennung und Beurteilung der Projektrisiken
2. Aufnahme und Beurteilung der Projektkontrollen
3. Analyse der verbleibenden Projektrisiken
4. Bewertung und Umsetzung von Maßnahmen
5. Laufende Verfolgung der Projektrisiken, -kontrollen und -maßnahmen

Bild 1 verdeutlicht den Zusammenhang der einzelnen Phasen für das Risikomanagement in IT-Projekten. Diese werden im folgenden besprochen.

Bild 1: Kreislauf des Projektrisikomanagements



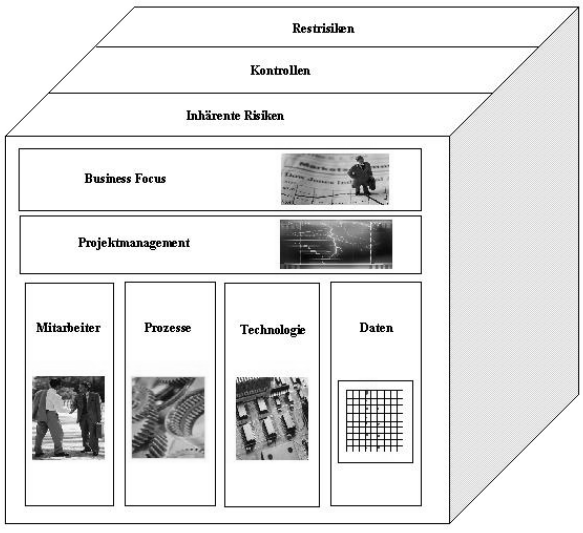
2.1 Projektrisiken erkennen und beurteilen

Herzstück eines effizienten Risikomanagements von IT-Projekten ist die systematische Sichtbarmachung der inhärenten Projektrisiken und die Beurteilung der vorhandenen Projektkontrollen. Projektrisiken sind mögliche Bedrohungen für den Erfolg eines Projektes. Inhärente Risiken sind Bedrohungen, die in einem Prozeß grundsätzlich existieren, d.h. bevor Kontrollen eingerichtet worden sind. Diese inhärenten Risiken hängen u.a. von der Art des Projektes, des Unternehmensbereiches und der eingesetzten Technologie ab. Die systematische Identifikation der inhärenten Projektrisiken sollte auf einem möglichst umfassenden Risikokatalog basieren, der die Erfahrungen aus vielen Projekten zusammenfaßt. Für eine solche Risiko-Checkliste wurde von mir eine Kategorisierung in die kritischen sechs Projektbereiche Projektmanagement, Business Fokus, Geschäftsprozesse, Anwender, Technologie und Daten vorgeschlagen [Ga02a].

Bild 2 (aus [Ga02b]) verdeutlicht die Dimensionen des Vorgehens für das Risikomanagement in IT-Projekten .

Damit eine solche Risiko-Checkliste einheitlich und personenunabhängig eingesetzt werden kann, sollten mehrere Leitfragen für jeden Projektbereich vorgegeben und jede Leitfrage durch Bewertungshinweise weiter erläutert werden. Eine Leitfrage im Projektbereich Technologie für das inhärente Projektrisiko „Neue Technologie“ lautet beispielsweise: „Hängt der Projekterfolg von Technologien ab, die neuartig sind und mit denen im Unternehmen wenig Erfahrung vorhanden ist?“ [Ga02a]. Ziel der Analyse ist, für jeden Projektbereich ein inhärentes Bereichsrisiko zu ermitteln, das in der folgenden Phase genauer bewertet wird.

Bild 2: Risikomanagement-Würfel



Die Beurteilung der Projektrisiken und –kontrollen erfolgt innerhalb der einzelnen Projektrisiko- und -kontrollbereiche primär qualitativ. Eine Einheitlichkeit der qualitativen

Risikobeurteilung wird durch Bewertungshinweise angestrebt. Zusätzlich werden für jeden Projektrisiko- und -kontrollbereich Beispiele für quantitative Risikoindikatoren eingesetzt. Als Risikoindikatoren im Projektrisikobereich „Technologie“ können beispielsweise die Anzahl der IT-Mitarbeiter im Projekt, die Anzahl der Schnittstellen zu anderen Anwendungen oder die Anzahl der verwendeten Programmiersprachen dienen. Grundsätzlich sollte beim Risikomanagement einer quantitativen Beurteilung zwar der Vorzug gegeben werden, allerdings ist eine verläßliche quantitative Beurteilung der Risiken von IT-Projekten extrem aufwändig. Die hier vorgestellte universell einsetzbare Vorgehensweise stellt daher einen praxisgerechten Kompromiß im Sinne eines Risikomanagement mit sich ergänzenden qualitativen und quantitativen Beurteilungsfaktoren dar.

2.2 Projektkontrollen aufnehmen und beurteilen

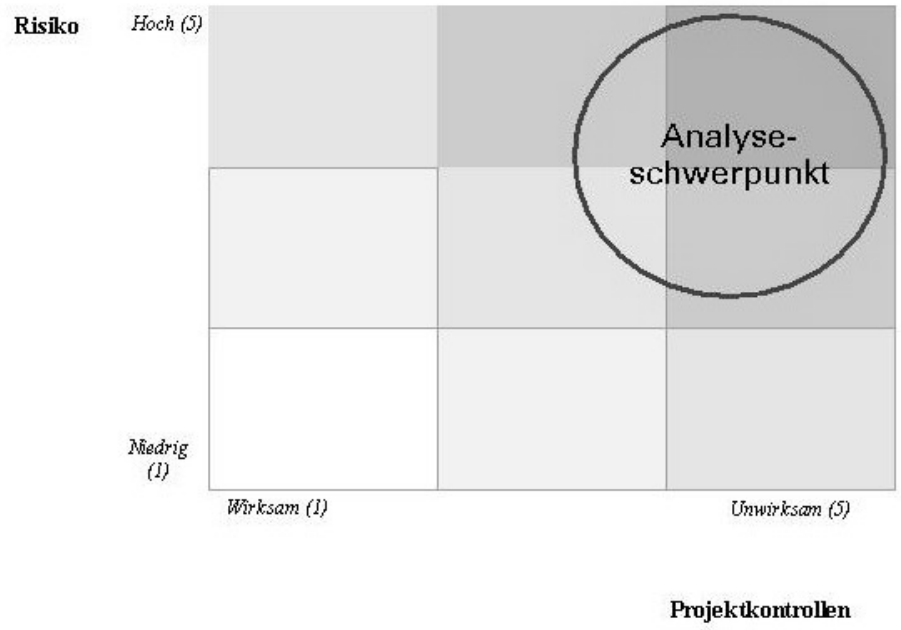
Zur Bewertung der Projektrisiken müssen die Kontrollen in den definierten kritischen Projektbereichen aufgenommen und deren Effektivität beurteilt werden. Die Erfassung und Beurteilung der Projektkontrollen muß natürlich ebenso systematisch erfolgen wie die Identifikation der Projektrisiken. Für jeden Projektbereich wird dazu anhand von Kontrollfragen und Best Practice-Beispielen die Effektivität der Projektsteuerungs- und kontrollverfahren bewertet. Im Projektbereich Technologie ist ein Vorgehensmodell beispielsweise eine allgemeine Projektkontrolle, die durch die Kontrollfrage „Erfolgt die Softwareentwicklung nach einem einheitlichen Vorgehensmodell?“ angesprochen wird [Ga02a]. Für die Bewertung der Effektivität dieses Projektkontrollverfahrens ist nicht allein die Existenz eines einheitlichen Vorgehensmodells entscheidend, sondern vor allem, ob dieses Vorgehensmodell auch durchgehend angewandt wird. Weitergehende Erläuterungen und Hinweise auf idealtypische Nachweise (zum Beispiel Dokumentation des Vorgehensmodells) für die einzelnen Kontrollfragen erleichtern eine genauere Beurteilung der Wirksamkeit der Projektkontrollen.

2.3 Verbleibende Projektrisiken analysieren

Durch die Abwägung von bewerteten inhärenten Risiken und existierenden Kontrollen kann das vorhandene Projektrisiko – je nach Bedarf – sowohl für jeden definierten kritischen Projektbereich als auch für jede einzelne Projektbedrohung ermittelt werden. Eine Risikoeinschätzung auf Ebene der Projektbereiche erlaubt in einem zweiten Durchgang eine fokussierte Analyse bzw. auf Ebene der einzelnen Projektbedrohungen die Definition und Umsetzung von Maßnahmen.

Die folgende Darstellung veranschaulicht die Analyse der bewerteten inhärenten Risiken und existierenden Kontrollen auf Ebene der Projektbereiche (Bild 3):

Bild 3: Analyse der verbleibenden Projektrisiken



2.4 Maßnahmen bewerten und ergreifen

Auf Basis der ermittelten Projektrisiken können in dieser Phase des Projektrisikomanagement-Prozesses gezielt Maßnahmen zur weiteren Risikominimierung festgelegt werden. Hilfreich bei der Priorisierung ist die Bildung eines Risiko-Faktors, der ein Produkt aus einem Maßstab (zum Beispiel 1=gering bis 5=sehr hoch) für die Eintrittswahrscheinlichkeit und für die Auswirkung / Schadenshöhe darstellt. Dieser Risikofaktor sollte vor dem Hintergrund der durchgeführten Risikoanalyse und in Diskussion mit den Projektverantwortlichen festgelegt werden, um aus wirtschaftlicher Sicht angemessene Maßnahmen einleiten zu können.

Bei der Festlegung der Maßnahmen kann man sich an der Systematik einer Risikoreduktions-Treppe orientieren [Ga02a], die aus den folgenden abgestuften Maßnahmen-Typen besteht:

- Risikovermeidung (zum Beispiel durch Änderung des Projektumfanges)
- Risikoverminderung (zum Beispiel durch Behebung der ermittelten Kontrollschwächen)
- Risikobegrenzung (zum Beispiel durch Entwicklung von Alternativen im Falle eines Scheitern des Projektes)
- Risikoverlagerung (zum Beispiel durch Vereinbarung von Schadensersatz)

- Risikoakzeptanz

Die Maßnahmen können – wie in Bild 4 dargestellt – nach Einschätzung der Schadenshöhe und der Wahrscheinlichkeit ausgewählt werden .

Bild 4: Auswahl der geeigneten Maßnahmen

Die festgelegten Maßnahmen müssen in den Projektplan integriert werden und sollten zusätzlich vom Risiko-Manager überwacht werden. Für die einzelnen Risiken sollte darüber hinaus ein Risiko-Eigentümer (Risk Owner) festgelegt werden, der auch für die Umsetzung der jeweiligen Maßnahmen und damit für die Bewältigung des Risikos verantwortlich ist.

2.5 Projektrisiken und Maßnahmen laufend überwachen

Eine einmalige Risikoaufnahme im IT-Projekt stellt kein ausreichendes Risikomanagement dar. Vielmehr sollte die Beurteilung der Risiken und Kontrollen über die gesamte Projektlaufzeit hinweg regelmäßig aktualisiert und ggf. weitere Maßnahmen definiert und umgesetzt werden. Ein hilfreiches Instrumentarium in diesem Zusammenhang ist die Definition und Überwachung des Risiko- und Kontrollniveaus mit Hilfe von Risiko- und Kontrollindikatoren, die ein objektives Maß für Veränderungen der Risiko- und Kontrollsituation darstellen. Im Projektbereich Technologie können beispielsweise die Anzahl der Programmzeilen, die Anzahl der Objekte, die Function Points oder die zyklomatische Zahl nach McCabe mögliche Risikoindikatoren für die Komplexität eines IT-Projektes sein [Ga02a].

Die Erfahrung zeigt, daß das Risikomanagement nicht in der Verantwortung des Projektleiters liegen sollte. Vielmehr sollte im Sinne eines 4-Augen-Prinzips und zur Vermeidung einer gewissen „Betriebsblindheit“ eine unabhängige Stelle regelmäßig den Status der Projektrisiken und -kontrollen überwachen.

3 Anwendung

Innerhalb der KPMG Deutsche Treuhand-Gesellschaft wird die dargestellte Vorgehensweise von dem Bereich Information Risk Management angewandt. Der Bereich Information Risk Management ist eine spezialisierte Einheit innerhalb der Wirtschaftsprüfungsgesellschaft KPMG, die sich mit der Prüfung und prüfungsnahen Beratung im Umfeld von IT-Systemen beschäftigt.

Mitarbeiter mit mindestens zwei bis dreijähriger Berufserfahrung werden im Rahmen eines 3-tägigen Kurses sowohl theoretisch als auch anhand einer Fallstudie mit der Vorgehensweise intensiv vertraut gemacht und dann auf entsprechenden Projekten bei Mandanten eingesetzt. Dabei hat sich die Skalierbarkeit der Vorgehensweise als ein großer Vorteil erwiesen. Projektrisikomanagement wird sowohl auf Ebene der Projektbereiche als „Project Quick Check“ als auch auf Ebene der Projekteinzelrisiken als „Project Review“ eingesetzt.

Der „Project Quick Check“ basiert in der Regel ausschließlich auf Interviews und erfolgt anhand eines zusammengefaßten Risikokataloges. Das Ergebnis wird in Form einer kurzen, grafischen Präsentation dargestellt, wobei als kritisch beurteilte Projektbereiche häufig noch einer weiteren Analyse bedürfen.

Beim „Project Review“ werden je nach Projekt verschiedene Methoden (u.a. Analyse von Projektdokumenten, Durchführung von moderierten Risiko-Workshops mit Kreativitätstechniken wie SWOT1-Analyse, Brainstorming oder Brainwriting, Befragung von ausgewählten Mitarbeitern in Interviews oder der mittels Fragebogen) eingesetzt. Bei Einsatz der Workshop- oder Interviewtechnik ist ein wichtiger Erfolgsfaktor für die Risikoerkennung erfahrungsgemäß die repräsentative Auswahl der Teilnehmer mit entsprechender vertikaler und horizontaler Abdeckung. Die vertikale Abdeckung bezieht sich dabei auf die Projekthierachie, die horizontale Abdeckung auf die Funktionalität. Bei der Beurteilung der vorhandenen Projektsteuerungs- und -kontrollverfahren kommen zusätzlich noch eigene Beobachtungen und Analysen zum Einsatz, da nur dadurch die Wirksamkeit der vorhandenen Projektkontrollen objektiv beurteilt werden kann. Das Ergebnis wird in der Regel in einer ausführlichen Präsentation mit detaillierten Maßnahmenempfehlungen dargestellt.

4 Ausblick

Die erfolgreiche Abwicklung von Projekten hat für die Wettbewerbsfähigkeit der Unternehmen eine strategische Bedeutung erlangt. Die meisten Projekte umfassen dabei wesentliche IT-Komponenten, da auch traditionelle Branchen ohne Informationstechnologie heutzutage nicht mehr lebensfähig sind und die Informationstechnologie sogar zum „Enabler“ für eine bessere Positionierung der Unternehmen im Wettbewerb geworden ist.

Das Thema Risikomanagement bei IT-Projekten hat für die Unternehmen aber nicht nur aufgrund der strategischen Bedeutung von IT an Bedeutung gewonnen, sondern auch weil die IT-Projekte immer anspruchsvoller und komplexer werden. Die Gründe dafür sind vielfältig:

[1] SWOT= Strength, Weaknesses, Opportunities, Threats

- Steigende Komplexität der Systeme und grenzüberschreitende Integration der IT-Strukturen durch Expansion / Globalisierung der Geschäftstätigkeit
- Zunehmende Systemintegration und weitgehende Automatisierung von Geschäftsprozessen durch zunehmenden Wettbewerbsdruck
- Steigende Abhängigkeit von der Verfügbarkeit und Sicherheit der Datenverarbeitung durch Öffnung der Unternehmenssysteme für Geschäftspartner und Kunden über das Internet
- Erhöhte Dynamik der Märkte durch neue Technologien, die neuartige Geschäftsprozesse (z.B. virtuelle Banken) ermöglichen
- Steigende Anforderungen des Gesetzgebers und der Aufsichtsbehörden (z.B. MaH, KonTraG, MaIR, Basel II)

Entsprechend werden insbesondere die mit der Durchführung von IT-Projekten verbundenen Risiken in Zukunft einen immer größeren Anteil der operativen Risiken in den Unternehmen darstellen und entsprechend ein systematisches Projektrisikomanagement unerläßlich werden.

Literaturverzeichnis

[BdB01] Bundesverband öffentlicher Banken Deutschlands (Hrsg.): Aktuelles – Ausgabe II/2001.

[Ga02a] Gaulke, M.: Risikomanagement in IT-Projekten. München - Wien 2002.

[Ga02b] Gaulke, M.: Management von operativen Risiken, URL: http://www.risikomanagement-in-it-projekten.de/Projektrisiken/Project_Risk_Review/project_risk_review.html, abgerufen am 03.07.2002, 12:00 Uhr.

[Ga02c] Gaulke, M.: Basel II, URL: http://basel2.markus-gaulke.de, abgerufen am 03.07.2002, 12:00 Uhr.

[HS87] Humphrey, W.S.; Sweet, W.L.: A Method for Assessing the Software Engineering Capability of Contractors; SEI Technical Report SEI-87-TR-23, Pittsburgh 1987.

[Jo99] Johnson, Jim: Turning Chaos into Success; in: Software Magazin, Dezember 1999.

[PMI00] Project Management Institute (Hrsg.): A Guide o the Project Management Body of Knowledge", Pennsylvania 2000.

[St99] Stienen, H.: Nach CMM und BOOTSTRAP: SPICE – Die neue Norm für Prozeßbewertungen; in: Industrie Management, Nr. 15, 1999.

[WSJ00] Tech-Project Inefficiencies Found in Corporate Study; in: The Wall Street Journal vom 14. November 2000, S. 20.