

Kleuker, Stephan; Ebrahim-Pour, Roya

Working Paper

Ein generisches Prozessmodell zur Einführung eines IT-Risikomanagement-Prozesses

Arbeitspapiere der Nordakademie, No. 2005-03

Provided in Cooperation with:

Nordakademie - Hochschule der Wirtschaft, Elmshorn

Suggested Citation: Kleuker, Stephan; Ebrahim-Pour, Roya (2005) : Ein generisches Prozessmodell zur Einführung eines IT-Risikomanagement-Prozesses, Arbeitspapiere der Nordakademie, No. 2005-03, Nordakademie - Hochschule der Wirtschaft, Elmshorn

This Version is available at:

<https://hdl.handle.net/10419/38587>

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.



ARBEITSPAPIERE DER NORDAKADEMIE

ISSN 1860-0360

Nr. 2005-03

Ein generisches Prozessmodell zur Einführung eines IT-Risikomanagement-Prozesses

Stefan Kleuker, Roya Ebrahim-Pour

November 2005

Eine elektronische Version dieses Arbeitspapiers ist verfügbar unter:
<http://www.nordakademie.de/index.php?id=ap>



Köllner Chaussee 11
25337 Elmshorn
<http://www.nordakademie.de>

Ein generisches Prozessmodell zur Einführung eines IT-Risikomanagement-Prozesses

Roya Ebrahim-Pour, Stephan Kleuker

1	EINLEITUNG	2
2	ANALYSE DER PROZESSREIFE VON UNTERNEHMEN	3
3	VORAUSSETZUNGEN FÜR DIE ERFOLGREICHE EINFÜHRUNG UND UMSETZUNG VON IT-RISIKOMANAGEMENT	7
4	RISIKOMANAGEMENT FÜR IT-PROJEKTE	8
5	DIE UMSETZUNG DES GENERISCHEN RM-PROZESSMODELLS	9
5.1	Prozessentwicklung	11
5.2	Prozessetablierung	12
6	FAZIT UND AUSBLICK	12
7	LITERATURVERZEICHNIS	14

Korrespondenzadressen:

Roya Ebrahim-Pour, NORDAKADEMIE – Hochschule der Wirtschaft, Köllner Chaussee 11, 25337 Elmshorn, Tel. 04121-409072, Fax: 04121-409040, Email: roya.ebrahim-pour@nordakademie.de

Prof. Dr. Stephan Kleuker, NORDAKADEMIE – Hochschule der Wirtschaft, Köllner Chaussee 11, 25337 Elmshorn, Tel. 04121-409041, Fax: 04121-409040, Email: s.kleuker@nordakademie.de

1 Einleitung

Risiken gehören zum Alltag der IT-Projekte. Der pro-aktive Umgang mit Risiken, d.h. ihre frühest mögliche Bearbeitung, ist jedoch in vielen Unternehmen nicht etabliert. Es gibt in den letzten Jahren immer mehr Unternehmen, die nach Lösungen suchen, IT-Projekte steuerbar, planbar und transparent zu gestalten [DeMarco, Lister 03]. Auch in der Literatur gibt es eine intensive Auseinandersetzung mit dem Thema und IT-Risikomanagement (IT-RM) wird als Lösung angeboten [Dorofee et al. 96], [Erben, Romeike 03], [Gaulke 02], [Kontio 97], [Versteegen 03], [Wallmüller 04]. Mit IT-RM gibt es die Chance Projekte in den gegebenen Rahmen durchzuführen und die geforderte Qualität zu erreichen, indem die Risiken in dem gesamten Lebenszyklus eines Projektes identifiziert und gesteuert werden.

In der Fachliteratur gibt es eine allgemeine und bis auf Details unumstrittene Vorgehensweise zu IT-RM mit den Arbeitsschritten Risikoidentifikation, -bewertung, -beherrschung und -überwachung, die allerdings im Detail nicht auf die individuellen Bedürfnisse der Unternehmen ausgerichtet ist. Der Versuch, RM in ein Unternehmen einzuführen, scheitert häufig, weil RM in die vorhandenen und spezifischen Prozesse eines Unternehmens integriert werden muss und diese verändert. Diese Prozesse sind Teil eines komplexen sozialen Umfeldes, das sich über die Zeit entwickelt hat und stark variieren kann. Ein erfolgreicher IT-RM-Prozess kann nur existieren, wenn er effektiv mit anderen Prozessen zusammenarbeitet. Daher wird ein generisches Prozessmodell benötigt, das für die vorhandenen Prozesse eines Unternehmens konkretisiert werden kann und dann auf Akzeptanz im Unternehmen stößt.

In dem Forschungsprojekt PAuR, Verbesserung der IT-Projektsachstandsverfolgung basierend auf Aufwandschätzungen und Risikomanagement, wird seit Januar 2004 mit 8 Industriepartnern untersucht, wie IT-RM in die Prozesse eines Unternehmens integriert werden kann. In [Kleuker, Ebrahim-Pour 05b] wurden die ersten Ergebnisse des Projektes veröffentlicht. Im Vordergrund standen die Themenabgrenzung, die theoretische Auseinandersetzung mit der Literatur im Bereich Risikomanagement und die ersten Ergebnisse der Zusammenarbeit mit den Partnerunternehmen. Um Wiederholungen zu vermeiden, werden wir uns in diesem Papier auf die neuen Ideen und Umsetzungskonzepte, die im Rahmen der praktischen Zusammenarbeit mit den Kooperationspartnern entstanden sind und die zugehörigen theoretischen Hintergründe konzentrieren.

Die Abbildung 1 stellt den RM-Einführungsprozess dar, der im Folgenden genauer erklärt wird. Bevor man über die Einführung von IT-RM nachdenkt, muss festgestellt werden, ob generell dokumentierte Prozesse im Unternehmen gelebt werden. Ist dies nicht der Fall, ist die alleinige Einführung von IT-RM keine sinnvolle Maßnahme. Die grundsätzlichen Randbedingungen zur Einführung von IT-RM werden im zweiten Kapitel beschrieben. Wenn eine IT-RM-Einführung grundsätzlich möglich ist, müssen weitere Randbedingungen bzgl. des Prozesses erfüllt sein, damit dieser erfolgreich umgesetzt werden kann. Diese Forderungen nach der Unterstützung durch die Unternehmensführung und den Aufbau einer Organisation zur Einführung des IT-RM-Prozesses werden im dritten Kapitel vorgestellt.

Die allgemeine Vorgehensweise zu IT-Risikomanagement wird im Kapitel 4 kurz zusammengefasst, damit im fünften Kapitel genauer beschrieben werden kann, welche generischen Schritte zu einer IT-RM-Umsetzung notwendig sind, die dann firmenindividuell konkretisiert werden müssen. Ein Fazit mit einem Ausblick schließt diese Arbeit im Kapitel 6 ab.

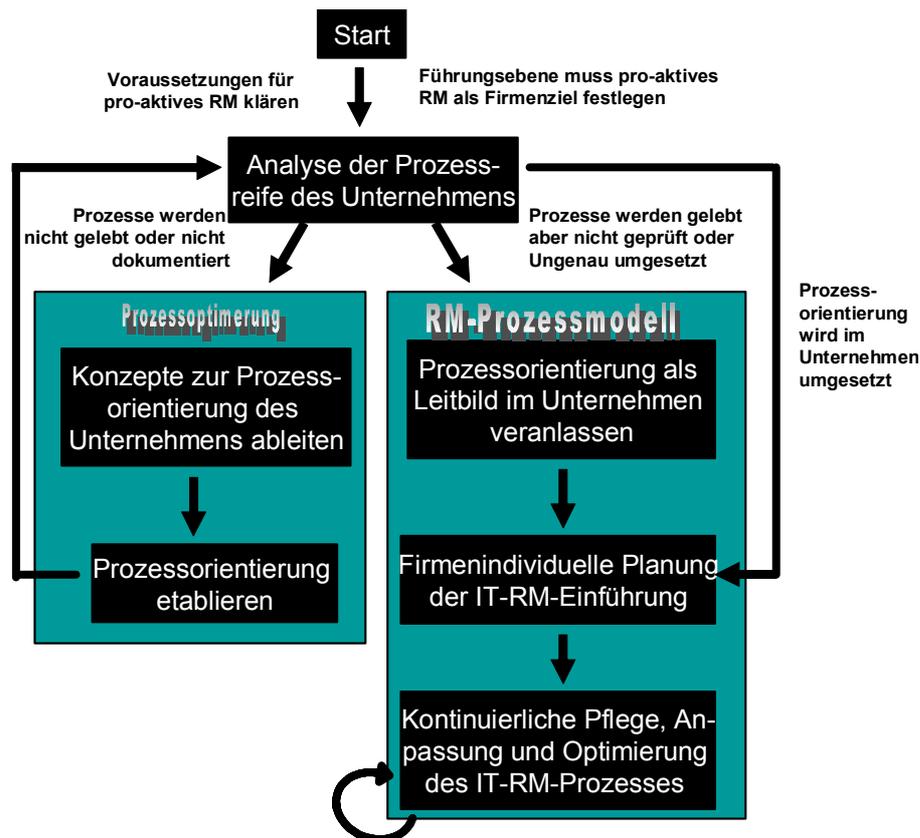


Abbildung 1: Das generische Prozessmodell für RM-Einführung

2 Analyse der Prozessreife von Unternehmen

Ausgehend von dem Wunsch IT-RM in einem Unternehmen zu etablieren, stellt sich die Frage ob die Umsetzung eines solchen Prozesses generell möglich ist. Unternehmen, in denen Prozesse nur dokumentiert sind, diese aber im täglichen Geschäft nicht oder sehr individuell umgesetzt werden, haben typischerweise Schwierigkeiten, einen neuen Prozess aktiv „zu leben“, da die Wahrscheinlichkeit, dass der neue Ansatz parallel zu anderen Ansätzen versandet, sehr groß ist.

Die Analyse der Prozessreife eines Unternehmens ist deshalb der erste Schritt, nachdem das pro-aktive RM zum Firmenziel erklärt wurde. Der Zweck dieser Untersuchung ist es, den

aktuellen Zustand der Firmenprozesse zu ermitteln. Je nach dem Ergebnis kann dann das weitere Vorgehen zur Einführung eines RM-Prozesses geplant werden.

Zentral stellt sich die Frage, wie das Unternehmen mit dem Thema Prozessorientierung umgeht. Dabei wird vorausgesetzt, dass eine qualitätsorientierte Ausrichtung des Unternehmens an dokumentierten, gelebten und gepflegten Prozessen als sinnvoll angesehen wird. Generell können sich die Prozesse eines Unternehmens in verschiedenen Zuständen befinden (siehe Abbildung 2), wobei in jedem Zustand ein bestimmter Umgang mit den Prozessen im Mittelpunkt des Interesses steht.

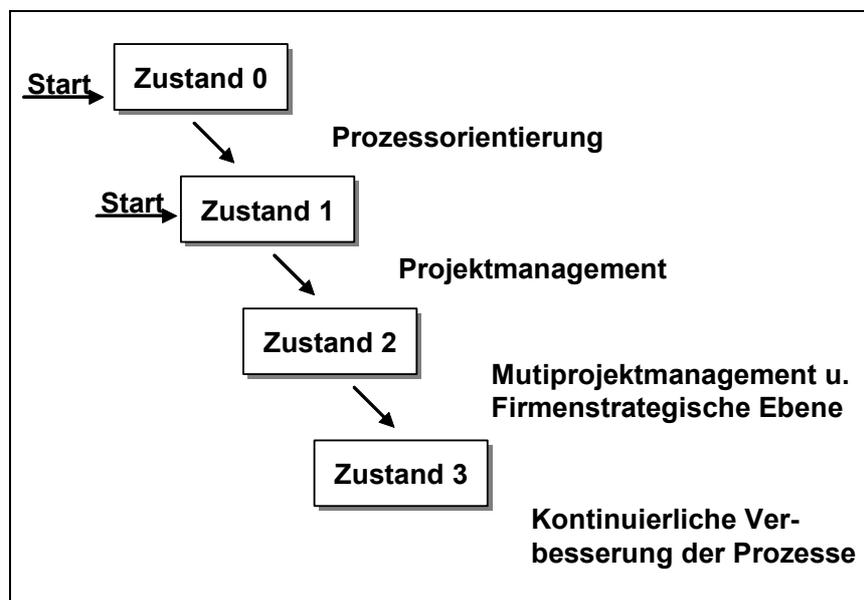


Abbildung 2: Prozessreifezustände eines Unternehmens

Zustand 0: Die Prozesse in dem Unternehmen sind nicht vordefiniert. Projekte laufen je nach Bedarf unterschiedlich. Der Erfolg oder Misserfolg von Projekten ist von Erfahrungen und dem Einsatz der Projektmitglieder abhängig. Insgesamt sind die Prozesse nicht aufeinander abgestimmt und es gibt keine oder geringe Erfahrungen mit vordefinierten Prozessen. Der Fokus bei dem Zustand 0 liegt auf der Prozessorientierung, das heißt, man versucht mit der Analyse der vorhandenen Prozesse des Unternehmens Ideen zu entwickeln, wie die Prozesse im Rahmen einer vordefinierten Vorgehensweise laufen können.

Zustand 1: Es gibt vordefinierte Prozessmodelle, die nur teilweise oder ungenau umgesetzt werden. Zwei Ziele stehen hier im Vordergrund: Verbesserung der Projektmanagementprozesse und die Institutionalisierung dieser Prozesse. Ohne ein funktionierendes Projektmanagement ist nicht an Veränderungen oder die Verbesserung der Prozesse zu denken. Die Projekte müssen geplant und die Umsetzung des Planung geprüft werden. Genau an dieser Stelle setzt das Risikomanagement an, das in die Projektmanagementprozesse integriert wird und für eine bessere Planung und Steuerung der Projekte sowie Transparenz in den Projekten sorgt.

Zustand 2: Die Projektmanagementprozesse sind eingespielt, Multiprojektmanagement zur Koordination verschiedener Projekte sowie die Prozesse auf firmenstrategischer Ebene sind nicht abgestimmt. Das Hauptziel in diesem Zustand ist es, Risikomanagement auf Multiprojektmanagement- und firmenstrategischer Ebene zu integrieren, um diese Prozesse in allen Firmenbereiche einheitlich umzusetzen.

Zustand 3: Risikomanagement ist Bestandteil der Prozesse auf allen Firmenebenen. Es gibt ein einheitliches Prozessmodell, das gelebt wird. Die kontinuierliche Verbesserung der Prozesse umfasst die ständige Pflege, Anpassung und Optimierung der Prozesse.

Die Unternehmen befinden sich beim Starten des Projektes RM-Einführung häufig entweder im Zustand 0 oder im Zustand 1. Zur Bestimmung der Prozessreife eines Unternehmens kann wie bei dem CMMI [CMMI 02], [Kneuper 02], an das das Zustandsmodell angelehnt ist, der Fragebogen aus der Abbildung 3 eingesetzt werden. Der Fragebogen ist nach verschiedenen Themenbereichen gegliedert, die einen Aufschluss über den Umgang mit Prozessen im Unternehmen, aber auch auf Projektebene ermöglichen. Das Ergebnis dieser Analyse bestimmt, welcher Arbeitsschritt als nächstes durchgeführt werden kann. Dabei deutet ein Ergebnis mit unter 25 Punkten häufig darauf hin, dass sich die Prozesse des Unternehmens im Zustand 0 befinden. Falls in einzelnen Bereichen die Punktzahl unter 4 ist, deutet dies drauf hin, dass hier maximal der Zustand 1 erreicht sein kann. Um den Zustand 3 zu erreichen, muss jede Frage zumindest mit zwei Punkten beantwortet worden sein.

Folgende nächste Schritte sind möglich:

- Allgemeine Prozessoptimierungen
Befinden sich die meisten Prozesse eines Unternehmens in den Zuständen 0 oder 1, müssen generelle Maßnahmen zur Prozessorientierung eingeleitet werden. Hierfür sind Konzepte zu erarbeiten, wie der Prozessgedanke im Unternehmen eingeführt werden kann und wie die interne Kommunikation über dokumentierte Prozesse zu verbessern ist. Die allgemeinen Prozessoptimierungen sind für die IT-RM-Einführung von großer Bedeutung, werden hier aber nicht weiterbehandelt, da sie als Teil einer Geschäftsprozessoptimierung und der Einführung eines Qualitätsmanagements, siehe z.B. [Deming 82] [Bartsch-Beuerlein 00], den Rahmen dieser Arbeit sprengen würden. Für einen Ansatz sei beispielhaft auf [Gadatsch 03] verwiesen.
- Anwendung des generischen RM-Prozessmodells
Wenn in einem Unternehmen prozessorientiert gearbeitet wird, die Prozesse aber nur teilweise oder ungenau umgesetzt werden, fördert und fordert das generische Prozessmodell die Umsetzung existierender Prozesse. Dabei steht dann im Vordergrund, die existierenden Prozesse mit dem IT-Risikomanagement zu verknüpfen und dieses kontinuierlich zu pflegen sowie zu optimieren.

Sind unsere Projekte reif für Risikomanagement?

Bewerten Sie folgende Aussagen für Ihr Unternehmen mit einer Punkteskala von 0 (trifft nicht zu) bis 3 (trifft voll zu). Wenn Sie weniger als 25 Punkte erreicht haben, sollten Sie neben der Einführung eines RM-Prozesses über allgemeine Prozessoptimierungen nachdenken.

❖ **Interne Kommunikation im Unternehmen**

- Die strategischen und taktischen Ziele des Unternehmens sind den Mitarbeitern bekannt.
- Neue Kundenverträge sind mit den betroffenen Abteilungen, die auch die Grenzen für Vertragsspielräume festlegen, abgesprochen.
- Für den Know-how-Transfer innerhalb des Unternehmens wird gesorgt, so dass der Ausfall einer Person (z.B. bei Krankheiten, Kündigungen etc.) die Planung nicht gefährdet.

❖ **Multiprojektmanagement**

- Es gibt ein Prozessmodell zur Koordination verschiedener Projekte, das in der Firma entwickelt wurde und gelebt wird.
- Es gibt ein definiertes Verfahren, wie neue Projekte in die Gesamtplanung mit ihren Anforderungen an Ressourcen aufgenommen werden.
- Es ist sichtbar, wann welche Mitarbeiter für welches Projekt arbeiten; in diese Planung sind Zeitpuffer aufgenommen.

❖ **Projektorganisation**

- Die Projektorganisation, d.h. die Verantwortlichkeiten, Kompetenzen und Berichtswege im Projekt sind klar definiert.
- Die Projektpläne werden während der Projektlaufzeit ständig aktualisiert, mit Kunden, den Unterauftragnehmern und dem eigenen Management durchgesprochen sowie Verzögerungen und mögliche Gegenmaßnahmen für potenzielle Probleme aufgenommen.
- Es gibt eine festgelegte Vorgehensweise für die Durchführung der Projekte.
- Es gibt eine festgelegte Vorgehensweise zur Messung der Produktqualität, des Projektfortschritts und für das Konfigurationsmanagement.

❖ **Entwicklungsprozesse**

- Anforderungen sind zu jedem Projektzeitpunkt klar definiert und das Team hat die Fähigkeit, diese zu bewältigen.
- Das Entwicklungsteam hat Erfahrungen mit den eingesetzten Techniken.
- Die Teammitglieder kennen den Entwicklungsprozess und können ihn umsetzen.

❖ **Qualitätsmanagement**

- Es gibt ein projektspezifisches und quantifiziertes Qualitätsmodell.
- Qualitätsmanagement ist integraler Bestandteil des Softwareentwicklungsprozesses.
- Es gibt definierte projektbezogene QM-Maßnahmen.
- Die Qualitätsmaßnahmen werden laufend überprüft.

❖ **Schnittstelle zum Kunden**

- Es gibt eine definierte und von allen Beteiligten akzeptierte Vorgehensweise zur Aufnahme neuer Kundenwünsche und ihrer Behandlung im Projekt.
- Der Abnahmeprozess durch den Kunden für die Projektergebnisse ist klar definiert.
- Es werden Abstimmungszeitpunkte mit Kunden vereinbart, um die offenen Fragestellungen zu klären und um den aktuellen Stand des Projektes mitzuteilen.

Abbildung 3: Fragebogen zur Bestimmung der Prozessreife des Unternehmens

3 Voraussetzungen für die erfolgreiche Einführung und Umsetzung von IT-Risikomanagement

Ist die Prozessorientierung Teil der Unternehmensphilosophie geworden, befinden sich also die meisten Prozesse des Unternehmens im zweiten Zustand, kann die konkrete Einführung eines IT-RM-Prozesses angegangen werden. Damit IT-RM erfolgreich in einem Unternehmen eingeführt kann, gibt es einige Voraussetzungen, die vorher erfüllt sein müssen. Die Klärung der Voraussetzungen hilft weiterhin allen Beteiligten zu erfahren, worauf man sich bei diesem Prozess einlässt und was zu beachten ist. Im Folgenden werden wichtige Randpunkte kurz skizziert. Weitere Details können [Kleuker, Ebrahim-Pour 05a] und [Kleuker, Ebrahim-Pour 05b] entnommen werden.

Die *volle Unterstützung des höheren Managements* ist vor dem Start des Projektes zu gewinnen. Das Management muss von den Ideen des RM grundsätzlich überzeugt sein und dahinter stehen.

Die *Partizipation der Mitarbeiter* ist die Voraussetzung dafür, dass neue Prozesse auch tatsächlich gelebt werden. Sinnvoll ist die Auswahl eines Kompetenzteams aus Projektmitarbeitern, Projektleitern, RM-Experten und Prozessexperten der Firma. In diesem Team müssen individuelle Erfahrungen aufgearbeitet werden, die dann in die firmenindividuelle Umsetzung des IT-RM-Prozesses einfließen.

Die *Verantwortlichkeiten* für die Prozessdurchführung, -umsetzung und -kontrolle sind im Vorwege zu klären. Dabei gilt es Personen zu unterscheiden, die für die Definition und Pflege des IT-RM-Prozesses und Personen, die für die Durchführung des Prozesses in den jeweiligen Projekten verantwortlich sind.

Das neue Wissen über die Neugestaltung der Prozesse muss in dem Unternehmen kommuniziert werden. *Prozessstraining* ist Bestandteil der Prozessetablierung für alle Unternehmensprozesse.

Die *Prozesskontrolle* ist ein wichtiger Bestandteil des Einführungsprozesses. Ob der neu definierte Prozess tatsächlich zum Einsatz kommt, kann damit beurteilt werden. Gerade in den ersten Einführungsphasen muss nicht nur geprüft werden, ob der Prozess gelebt wird, es muss weiterhin festgestellt werden, ob frühzeitig Änderungen am Prozess notwendig sind, da eventuell bestimmte Randbedingungen bei der Prozessentwicklung nicht berücksichtigt wurden.

Risikokultur ist ein Teil der Unternehmenskultur, die das Risikobewusstsein und -handeln fördert, in der offen über Risiken kommuniziert werden kann. Diese Kultur wächst schrittweise im Rahmen des Einführungsprozesses.

4 Risikomanagement für IT-Projekte

Bevor die weiteren Schritte zur generischen Einführung eines IT-RM-Prozesses erläutert werden, ist es sinnvoll die zentralen Begriffe des RM in der Form zu definieren, wie sie in diesem Artikel genutzt werden. Die benutzten Definitionen lehnen sich dabei sehr eng an verschiedene Werke (vgl. [DeMarco, Lister 03], [Erben, Romeike 03], [Gaulke 02], [Versteegen 03], [Wallmüller 04]) zum Thema RM an.

Bevor die Begriffe des RM geklärt werden, ist festzuhalten, was hier unter IT-Projekten verstanden wird, auf die dann der IT-RM-Prozess angewandt werden kann. Der Begriff IT-Projekt umfasst Projekte, deren Ergebnisse unmittelbar im Zusammenhang mit der IT stehen. Dies sind Projekte mit folgenden Schwerpunkten:

- Software (SW)-Entwicklung, d.h. Neuentwicklung, Anpassung und Erweiterung für externe oder interne Kunden
- Fremdvergabe eines SW-Entwicklungsauftrages an einen Auftragnehmer; dies beinhaltet die Auftragssteuerung
- Anpassungen und Erweiterungen der IT-Infrastruktur für externe oder interne Kunden

Risikomanagement für IT-Projekte ist eine gesunde Mischung aus optimistischen Einstellungen, sich den neuen komplexen Aufgabenstellungen stellen zu wollen, und die potentiellen Gefahren ernst zu nehmen, um sie dann systematisch anzugehen. Ursache für das Scheitern von vielen IT-Projekten ist das Verdrängen von externen und internen Randbedingungen, die Bestandteil aller komplexen Projekte sind und die Ergebnisse der Projekte stark beeinflussen können. IT-RM beinhaltet alle systematischen Maßnahmen zur rechtzeitigen Erkennung, Bewertung und Steuerung der potenziellen Risiken in IT-Projekten. In der Abbildung 4 ist die allgemeine Vorgehensweise des RM dargestellt:

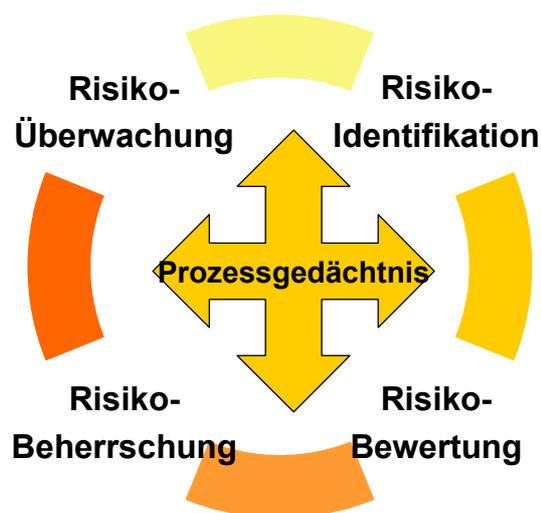


Abbildung 4: Allgemeine Vorgehensweise beim RM

Die *Risikoidentifikation* dient dem Herausarbeiten von potenziellen Risiken und ist damit der wichtigste Arbeitsschritt von RM. Wenn Risiken nicht identifiziert sind, bleibt auch deren Planung bzw. Steuerung aus. Zur Entdeckung von Risiken können verschiedene Methoden wie Fragebögen, Interviews, Brainstorming oder eine Szenariotechnik herangezogen werden. Auch eine Kombination der Methoden ist empfehlenswert. Das Ergebnis der Risikoidentifikation ist eine Risikoliste, die alle potenziellen Risiken enthält.

Die *Risikobewertung* ist der nächste Arbeitsschritt, der auf der Risikoliste aufsetzt und zu jedem Risiko eine Bewertung liefert. Die Experten geben Schätzungen über die Eintrittswahrscheinlichkeit und die Schadenshöhe eines Risikos, wenn es eintritt, ab. Aus der Multiplikation der beiden Werte entsteht ein quantitativer Wert, mit dem eine Priorisierung der Risiken vorgenommen werden kann.

Die *Risikobeherrschung* ist die Maßnahmenplanung für die wichtigsten Risiken, die das Ergebnis eines Projektes negativ beeinflussen können. Die unterschiedlichen Strategien zur Schadensbegrenzung sind Risikominimierung, Verlagerung oder Versicherung gegen das Risiko. Je nach Kontext des Projektes kann über die geeignete Strategie entschieden werden. Zu beachten ist, dass die Maßnahmen nicht die Kosten, die ein Risiko verursachen kann, überschreiten dürfen. Ein Teilaspekt ist dabei, dass bestimmte Werte, wie die Rufschädigung für ein Unternehmen, nur schwer in einem quantitativen Wert ausgedrückt werden können.

Die *Risikoüberwachung* ist der letzte Arbeitsschritt in einem RM-Zyklus und umfasst die Beobachtung der Entwicklung des Risikos und des Erfolgs der Gegenmaßnahmen. Diese Daten werden auch zum Aufbau einer Historie von Risiken genutzt.

Insgesamt handelt es sich dabei um einen zyklischen Prozess, dabei wird zu verschiedenen Zeitpunkten, wie Projektmeilensteinen, die Risikoidentifikation immer wieder zur Entdeckung neuer Risiken genutzt. Durch die Dokumentation der Entwicklung der Risiken und der zugehörigen Maßnahmen kann schrittweise ein Prozessgedächtnis z.B. in der Form einer Datenbank oder einer Wissensmanagement-SW aufgebaut werden, das das Wissen und die Erfahrungen von Projekten in sich trägt. Andernfalls geht dieses Wissen meist verloren, sobald Personen das Unternehmen verlassen oder ausfallen. Die Informationen und das Wissen werden so unternehmensweit verfügbar gemacht. Durch eine genaue Analyse der Risiken unterschiedlicher Projekte in einer solchen Wissensbasis ist es weiterhin möglich, generelle Ursachen von Risiken zu erkennen. Gibt es z.B. viele sehr ähnlich lautende Risiken kann dies ein wichtiger Indikator dafür sein, dass ein Unternehmensprozess optimiert werden sollte.

5 Die Umsetzung des generischen RM-Prozessmodells

Nachdem im vorherigen Kapitel die allgemeine Vorgehensweise beim RM beschrieben wurde, stellt sich die Frage, wie die Umsetzung dieser Vorgehensweise unter Berücksichtigung der firmenindividuellen Prozesse konkret aussehen kann. Das generische Prozessmodell für IT-RM gibt dabei einen Rahmen vor, der entsprechend den aktuellen Bedürfnissen des Unternehmens unterschiedlich ausgearbeitet werden muss.

Damit dieses Modell tatsächlich umgesetzt wird, ist die Entwicklung und Gestaltung des RM-Prozesses von wesentlicher Bedeutung. Auch wenn größere Unternehmen oft spezielle Abteilungen für die Definition von Vorgehensmodellen haben, ist es wichtig, Mitarbeiter aus unterschiedlichen Ebenen (Projektleiter, Projektmitarbeiter, Fachleute für Definition von Methoden usw.) an diesem Prozess zu beteiligen. Der Vorteil dieser Herangehensweise ist, dass durch die Mitarbeiterbeteiligung mit einer höheren Akzeptanz des Modells zu rechnen ist. Die aktive Mitarbeit von Personen aus verschiedenen Ebenen fördert den Teamgeist und die bereichsübergreifende Zusammenarbeit im Unternehmen. Darüber hinaus werden wertvolle Informationen und Erfahrungen über den Verlauf von früheren Projekten gesammelt, die auf dieser Weise herausgearbeitet werden können. Dieses Wissen bildet den ersten Input für das Prozessgedächtnis, das im Rahmen eines integrierten Risikomanagementprozesses aufgebaut wird.

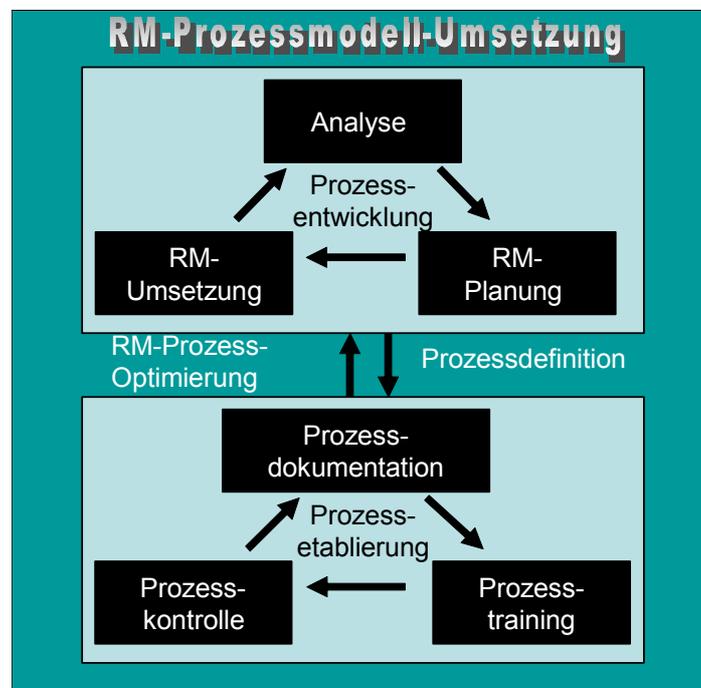


Abbildung 5: Umsetzung des generischen Prozessmodells

Der Umsetzungsprozess von RM besteht generell aus der Prozessentwicklung und der Prozessetablierung (vgl. Abbildung 5). Ziel der Prozessentwicklung ist es, Ideen zu entwickeln, wie Risikomanagement in die Prozesse des Unternehmens integriert werden kann und diese dann umzusetzen. In der Prozessetablierung geht es darum, den entwickelten Prozess zu leben, diese Umsetzung zu kontrollieren und aus dem Einsatz des Prozesses Optimierungsmöglichkeiten zu erkennen. Zwischen Prozessentwicklung und Prozessetablierung gibt es einen Austausch von Informationen. Die Ergebnisse der Prozessentwicklung fließen in Form der Prozessdefinition in die Prozessetablierung, damit diese als einheitliches Vorgehensmodell für das Unternehmen genutzt werden kann. Die Ergebnisse der Prozessetablierung geben wertvolle Rückmeldungen zu den Prozessoptimierungen, die erneut erprobt werden können.

5.1 Prozessentwicklung

In der Zusammenarbeit mit den Partnerunternehmen des Projektes hat sich das Veranstellen von Workshops als ein sinnvolles Hilfsmittel für die Prozessentwicklung bewährt. Dabei stehen folgende Arbeitsschritte an:

- Analyse
Mit der Analyse der früheren Projekte gibt es aufschlussreiche Informationen über den Verlauf der Projekte, deren Risiken und wie sie gegebenenfalls gemeistert wurden. Das Ziel ist es, Informationen über die möglichen Problemquellen bzw. Risiken zu gewinnen und durch die Offenlegung der Risiken eine Kultur des Risikobewusstseins und des risikoorientierten Handelns zu schaffen. Die ermittelten Risiken werden verschiedenen Themenbereichen, wie z.B. Projektmanagement, Multiprojektmanagement, Zusammenarbeit mit Kunden, externe Auftragnehmer und Firmenprozesse zugeordnet.
- RM-Planung
Die Risikoquellen bilden die erste Grundlage für die Planung der Einbindung des Risikomanagements. Dabei gibt es zwei Klassen von Risiken:
 - statische Risiken, deren Ursachen in den Prozessen des Unternehmens liegen. Diese Risiken tauchen immer wieder bei verschiedenen IT-Projekten auf und sind aus dem Projektumfeld nicht sinnvoll behandelbar. Sie können nur im Rahmen allgemeiner Prozessoptimierungen angegangen werden.
 - dynamische Risiken hingegen sind individuelle Projektrisiken, die zwar in verschiedenen Projekten auftauchen können, aber immer mit dem individuellen Kontext des Projektes im engen Zusammenhang stehen. Mit einem funktionierenden RM-Prozess können Schritte geplant werden, um die Folgen dieser Risiken zu verringern oder sie gar aus der Welt zu schaffen.

Es ist sinnvoll, jedes Risiko einer Klasse zuzuordnen. Mit den statischen Risiken entwickeln sich Denkanstöße für eine allgemeine Prozessverbesserung, die parallel zu der RM-Prozesseinführung durchgeführt werden kann.

Bei den dynamischen Risiken wird in der Gruppe diskutiert, welche Projektabläufe betroffen sind. Normalerweise sind es Projektmanagement-, Aufwandsschätzung- und Controllingabläufe. Hier entstehen Ideen zur Integration von RM in die vorhandenen Prozesse des Unternehmens. Insgesamt entsteht so eine Grundlage, welche Risikogebiete in dem Unternehmen systematisch in jedem Projekt erfasst werden sollten und wie Informationen über Risiken über verschiedene Prozessgrenzen hinaus fließen können.

- RM-Umsetzung
Die Umsetzung der Ideen für die Integration von RM kann im Rahmen eines Pilotprojektes erprobt werden. Dazu werden die Informationen aus der Planung in einer Prozessdefinition aufbereitet, die den an die unternehmensindividuellen Gegebenheiten angepassten RM-Prozess mit seiner unternehmensindividuellen Einbettung in die existierenden Prozesse beschreibt. Empfehlenswert als Pilotprojekte sind Projekte, die zwar für die Problemstellung maßgebend sind, aber nicht unter enormem Zeitdruck stehen.

5.2 Prozessetablierung

Die Prozessetablierung umfasst alle Aktivitäten zur Institutionalisierung der erprobten Prozesse in einem Unternehmen und basiert auf den Ergebnissen der Prozessentwicklung.

- Prozessdokumentation
Die Prozessdefinition ist die Beschreibung des RM-Prozesses und seiner Schnittstellen als allgemeine Vorgehensweise für ein Unternehmen. Teil der Definition sind Angaben darüber, welche Konkretisierungen bzw. Prozessanpassungen in individuellen Projekten gemacht werden können. Ein Teilergebnis ist die Prozessdokumentation, in der das projektindividuelle Vorgehen und später die Prozessergebnisse festgehalten werden.
- Prozesstraining
Damit eine einheitliche Vorgehensweise unternehmensweit zum Einsatz kommen kann, muss das Wissen darüber innerhalb der Firma trainiert werden. Denn nur wenn die Mitarbeiter Kenntnisse über das Vorgehensmodell haben, können sie diese auch für die Abwicklung der aktuellen Projekte einsetzen. Erkenntnisse des Trainings können unmittelbar in projektindividuelle Workshops einfließen, in denen die Risikoidentifikation durchgeführt wird.
- Prozesskontrolle
Die Prozesskontrolle enthält die Kontrolle der Einhaltung der Prozessmodelle auf der einen Seite und Ermittlung der Probleme des Prozessmodells auf der anderen Seite. Werden Probleme identifiziert, fließen diese bei kleineren Problemen in die dann anzupassende Prozessdefinition oder bei größeren Problemen zur Prozessentwicklung, in der über Veränderungen des Modells nachgedacht werden muss.

6 Fazit und Ausblick

Generell gibt es eine allgemeine, leicht verständliche und anerkannte Vorgehensweise, wie Risikomanagement in IT-Projekten durchgeführt werden kann. Leider bereitet die Umsetzung dieses theoretischen Ansatzes zusammen mit den vorhandenen Prozessen eines Unternehmens Probleme, die auf die Individualität und Komplexität dieser Prozesse zurückzuführen ist.

Daraus folgt zunächst, dass die konkrete Einführung eines RM-Prozesses unternehmensindividuell gestaltet werden muss. Betrachtet man unterschiedliche Umsetzungen kann man sich dann der Frage stellen, ob diese Ansätze Gemeinsamkeiten haben. Diese Gemeinsamkeiten

wurden hier als Teilergebnis des Forschungsprojekts PAuR in ein generisches Prozessmodell zur Einführung eines IT-RM-Prozesses zusammengefasst.

Weiterhin wurde gezeigt, dass vor der eigentlichen Umsetzung der theoretischen Ansätze des IT-RM bereits geklärt werden muss, ob die Prozesseinführung grundsätzlich erfolgreich sein kann.

Deshalb basiert das generische Prozessmodell zur Einführung und Umsetzung des IT-RM-Prozesses darauf, dass die Prozesserneuerungen aus dem bereits prozessorientiert arbeitenden Unternehmen heraus wachsen müssen, damit der Prozess von den Mitarbeitern akzeptiert und gelebt wird und die Erfahrungswerte in dem Unternehmen nicht verloren gehen.

Die Umsetzung des RM ist mit den zwei Aktivitäten Prozessentwicklung und -etablierung verbunden. Die beiden Aktivitäten stehen in einem ständigen Austausch, um Prozessoptimierungsideen zu erproben und die erprobten Prozesse zu dokumentieren und umzusetzen. Insgesamt ist die IT-RM-Einführung ein Schritt zur Optimierung der Prozesse eines Unternehmens, insbesondere auf dem Gebiet des Projektmanagements.

In zukünftigen Arbeiten kann untersucht werden, ob die generischen Anteile des vorgestellten Ansatzes weiter konkretisiert werden können, ohne den generischen Anspruch zu verlieren. In den vorhergehenden Kapiteln wurde bereits angedeutet, dass es einige Themengebiete gibt, die in fast allen Unternehmen eine zentrale Bedeutung haben. Diese Gebiete kann man systematisch erfassen und so zu einer Verfeinerung des ursprünglichen Ansatzes beitragen.

Weiterhin kann untersucht werden, ob der Übergang zwischen einer unternehmensweit gültigen Prozessdefinition zu einer projektindividuellen Umsetzung weiter konkretisiert werden kann. Dazu sind Gemeinsamkeiten von Projekten zu identifizieren, die in die konkrete Anpassung eines Projekts einfließen können.

Eine generische Aufbereitung der Möglichkeiten, den Erfolg von Maßnahmen gegen Risiken zu beurteilen und bei zwei möglichen Maßnahmen die wahrscheinlich erfolgreichere auszuwählen ist zunächst anhand praktischer Beispiele und dann eines dahinter liegenden mathematischen Modells aufzubereiten. Dabei stellt sich die Frage, wie der Erfolg einer Maßnahme kurzfristig aber auch langfristig beurteilt werden kann.

Die angedeutete Verknüpfung der Nutzung des RM-Prozesses auf Projektebene mit dem RM auf Multiprojekt- oder Unternehmensebene kann ebenfalls als Erweiterung des generischen Modells betrachtet werden.

Insgesamt zeigt sich, dass man ausgehend von dem Wunsch einen theoretischen Ansatz unternehmensindividuell umzusetzen, durch Abstraktion zu einem wertvollen generischen Modell zur Umsetzung kommen kann, das in folgenden Forschungsarbeiten auf generischer Ebene weiter konkretisierbar ist.

7 Literaturverzeichnis

- [Abdomerovic 04] Muhamed Abdomerovic, Brainstorming the PMBOK Guide, Pennsylvania: Project Management Publications, 2004
- [Balzert 98] Helmut Balzert, Lehrbuch der Software-Technik - Software-Management, Software-Qualitätssicherung, Unternehmensmodellierung, Heidelberg; Berlin: Spektrum Akademischer Verlag, 1998
- [Bartsch-Beuerlein 00] Sandra Bartsch-Beuerlein, Qualitätsmanagement in IT-Projekten, München; Wien: Carl Hanser Verlag, 2000
- [Bieta et al. 02] Volker Bieta, Johannes Kirchhoff, Hellmuth Milde, Wilfried Siebe, Risikomanagement und Spieltheorie, Bonn: Galileo Business, 2002
- [Boehm 89] Berry Boehm, Software Risk Management, IEEE Computer Society Press, 1989
- [Burghardt 02] Manfred Burghardt, Projektmanagement – Leitfaden für die Planung, Überwachung und Steuerung von Entwicklungsprojekten, 6. überarbeitete Auflage, Erlangen: Publicis Corporate Publishing, 2002
- [CMMI 02] CMMI Product Team, Capability Maturity Model® Integration (CMMISM), Version 1.1, CMU/SEI-2002-TR-011, ESC-TR-2002-011, Carnegie Mellon University, 2002
- [DeMarco 98] Tom DeMarco, Der Termin, München; Wien: Carl Hanser Verlag, 1998
- [DeMarco 01] Tom DeMarco, Spielräume - Projektmanagement jenseits von Burn-out, Stress und Effizienzwahn, München; Wien: Carl Hanser Verlag, 2001
- [DeMarco, Lister 03] Tom DeMarco, Timothy Lister, Barentango - Mit Risikomanagement Projekte zum Erfolg bringen, München; Wien: Carl Hanser Verlag, 2003
- [Deming 82] W. Edwards Deming, Quality, Productivity, and Competitive Position, Massachusetts Institute of Technology, 1982

- [DIN 04] Qualitätsmanagement – Verfahren, DIN-Taschenbuch 226, 5. Auflage, Berlin; Wien; Zürich: Beuth Verlag, 2004
- [Dorofee et al. 96] Audrey J. Dorofee, Julie A. Walker, Christopher J. Alberts, Ronald P. Higuera, Richard L. Murphy, Ray C. Williams, Continuous Risk Management Guidebook, Carnegie Mellon University, 1996
- [Emam et al. 97] Khaled El Emam (Hrsg.), Walcelio Melo (Hrsg.), Jean-Normand Drouin (Hrsg.), Spice: The Theory and Practice of Software Process Improvement and Capability Determination, New York: John Wiley & Sons, 1997
- [Erben, Romeike 03] Roland Erben, Frank Romeike, Allein auf stürmischer See, Risikomanagement für Einsteiger; Weinheim: WILEY-VCH, 2003
- [Gadatsch 03] Andreas Gadatsch, Grundkurs Geschäftsprozess-Management, 3. Auflage, Wiesbaden:Vieweg, 2003
- [Gaulke 02] Markus Gaulke, Risikomanagement in IT-Projekten, München; Wien: R. Oldenbourg Verlag, 2002
- [Guldentops, De Haes 02] Erik Guldentops, Steven De Haes, COBIT 3rd Edition Usage Survey: Growing Acceptance of COBIT, in: Information Systems Control Journal, 2002, Vol. 6, Seiten 25–31.
- [Hofmann 02] Gerhard Hofmann, Basel II und MaK – Vorgaben, bankinterne Verfahren, Bewertungen, Frankfurt am Main: Bankakademie-Verlag, 2002
- [Kleuker, Ebrahim-Pour 04] Stephan Kleuker, Roya Ebrahim-Pour, Chancen nutzen, IT-Projekte erfolgreich abzuwickeln, in: campusforum (<http://www.nordakademie.de>), Nr. 11 / Juni 2004
- [Kleuker, Ebrahim-Pour 05a] Stephan Kleuker, Roya Ebrahim-Pour, Integration eines IT-Risikomanagementprozesses in laufende Firmenprozesse, in: RISKNEWS – Das Fachmagazin für Risikomanagement, 01/2005

- [Kleuker, Ebrahim-Pour 05b] Stephan Kleuker; Roya Ebrahim-Pour, Ein pragmatischer Ansatz zur individuellen Integration vom IT-Risikomanagement in Unternehmen, Arbeitspapiere der NORDAKADEMIE, ISSN 1860-0360 (<http://www.nordakademie.de/index.php?id=ap>)
- [Kleuker, Ebrahim-Pour 05c] Stephan Kleuker, Roya Ebrahim-Pour, Sind Ihre Projekte reif für Risikomanagement, in: campusforum (<http://www.nordakademie.de>), Nr. 15 / Juni 2005
- [Kneuper 02] Ralf Kneuper, CMMI, Heidelberg: dpunkt.verlag, 2002
- [Kontio 97] Jyrki Kontio, The Riskit Method for Software Risk Management, Version 1.0, CS-TR-3782/UMIACS-TR-97-38, University of Maryland, 1997
- [PMI 00] Project Management Institute (Hrsg.), A Guide to the Project Management Body of Knowledge (PMBOK Guide), Ausgabe 2000, Pennsylvania: Project Management Publications, 2000
- [Stienen 99] Hans Stienen, Nach CMM und BOOTSTRAP: SPiCE. Die neue Norm für Prozessbewertungen, in: INFORMATIK / INFORMATIQUE:(Zeitschrift der schweizerischen Informatik Organisation), 6/1999
- [Versteegen 02] Gerhard Versteegen (Hrsg.), Software-Management: Beherrschung des Lifecycles, Berlin; Heidelberg: Springer-Verlag, 2002
- [Versteegen 03] Gerhard Versteegen (Hrsg.), Risikomanagement in IT-Projekten, Berlin; Heidelberg: Springer-Verlag, 2003
- [Wallmüller 04] Ernest Wallmüller, Risikomanagement für IT- und Software-Projekte, München; Wien: Carl Hanser Verlag, 2004
- [Weltz, Ortmann 92] Friedrich Weltz, Rolf G. Ortmann, Das Softwareprojekt - Projektmanagement in der Praxis, Frankfurt; New York: Campus Verlag, 1992

Arbeitspapiere der NORDAKADEMIE

Bisher erschienen sind:

2005-03	Stephan Kleuker Roya Ebrahim-Pour	Ein generisches Prozessmodell zur Einführung eines IT-Risikomanagement-Prozesses
2005-02	Ralf Kesten	ERIC versus EVA: Zwei wertorientierte Controllingkennzahlen im kritischen Vergleich
2005-01	Stephan Kleuker Roya Ebrahim-Pour	Ein pragmatischer Ansatz zur individuellen Integration von IT-Risikomanagement in Unternehmen
2004-04	Axel Dreher Tim Krieger	Do gasoline prices converge in a unified Europe with non-harmonized tax rates?
2004-03	Ralf Kesten	Controlling von Projektbudgets mit Earned Value Analysen
2004-02	Arno Müller, Lars von Thienen, Hinrich Schröder	IT-Controlling : So messen Sie den Beitrag der Informationstechnologie zum Unternehmenserfolg
2004-01	Tim Krieger	Public pensions and immigration policy when voters are differently skilled