Leseprobe

Risikomanagement in IT-Projekten von Markus Gaulke, 2., überarbeitete Auflage

ISBN: 3486275992

Quelle: www.risikomanagement-in-it-projekten.de

Inhalt

1 Vorwort 6

1.1 Vorwort zur 2. komplett neubearbeiteten Auflage ... 6

1.2 Vorwort zur 1. Auflage ... 7

2 Einführung 10

2.1 Grundlegende Begriffe ... 10

2.1.1 Projekt ... 10

2.1.2 Risiko ... 12

2.1.3 Projektrisiko ... 13

2.1.4 Risikomanagement ... 15

2.2 Risikomanagement bei IT-Projekten ... 17

3 Notwendigkeit für ein Risikomanagement bei IT-Projekten 19

3.1 Gesetzliche und aufsichtliche Anforderungen ... 21

3.1.1 Corporate Governance und IT-Governance ... 21

3.1.2 KonTraG ... 25

3.1.3 Mindestanforderungen an das Betreiben von Handelsgeschäften ... 26

3.1.4 Besondere organisatorische Pflichten von Instituten ... 27

3.1.5 OCC Technology Risk Management ... 27

3.1.6 Basel II ... 30

3.2 Best Practice ... 32

3.2.1 CMM ... 32

3.2.2 BOOTSTRAP ... 34

3.2.3 ISO 15504 (SPICE) ... 35

3.2.4 Project Management Institute ... 35

3.2.5 U.K. Association for Project Management ... 37

3.2.6 DIN 62198: Risikomanagement für Projekte ... 37

3.2.7 COBIT ... 39

3.2.8 SEI Risk Taxonomy ... 41

3.2.9 CCTA Risk Handbook ... 42

3.2.10 DriveSPI ... 45

3.3 Real Practice ... 46

3.3.1 Chaos-Studie ... 47

3.3.2 TechRepublic-Studie ... 48

3.3.3 IT-Kosten und IT-Performance 2002 ... 48

4 Ursachen für Projektfehlläufer und Erfolgsfaktoren 49

4.1 Studien ... 49
4.1.1 KPMG-Studie: “IT Runaway Systems” ... 49
4.1.2 The Standish Group: “Chaos” ... 51
4.1.3 KPMG-Studie: “What went wrong?” ... 52
4.1.4 Computerwoche-Befragung ... 52
4.1.5 Daily Telegraph-Studie ... 53
4.1.6 Forsa-Befragung ... 54
4.1.7 Softwareentwicklung in Deutschland ... 54
4.1.8 Droege & Comp.-Befragungen ... 55
4.1.9 KPMG: “Programme Management Survey” ... 56
4.2 Expertenmeinungen ... 56
4.2.1 Erfahrungen eines externen IT-Dienstleisters ... 57
4.2.2 Projektrisiken bei einem CMM Level 4-Unternehmen ... 57
4.2.3 Prinzipien erfolgreicher Großprojekte ... 58
4.2.4 Zwölf klassische Projektfehler und zehn Erfolgsfaktoren ... 59
4.2.5 Grundprinzipien der Softwareentwicklung ... 61

5 Kurzdarstellung der Vorgehensweise 63

5.1 Methodik ... 63
5.2 Struktur ... 66
5.3 Anwendung ... 68

6 Projektrisiken erkennen und beurteilen 70

6.1 Vorgehensweise ... 70
6.1.1 Projektrisiken erkennen ... 70
6.1.2 Projektrisiken beurteilen ... 72
6.2 Geschäftliche Ausrichtung ... 74
6.2.1 Fehlende geschäftliche Unterstützung ... 74
6.2.2 Mangelnde Stabilität der Organisation ... 75
6.2.3 Hohe Dynamik des Marktumfeldes ... 76
6.2.4 Kritikalität des IT-Systems ... 77
6.2.5 Außergewöhnliche Risiken ... 78
6.2.6 Projektrisiko-Checkliste ... 78
6.2.7 Projektrisikoindikatoren ... 79
6.3 Projektmanagement ... 82
6.3.1 Fehlende Erfahrung und Sachkenntnis ... 83
6.3.2 Mangelnde Ressourcen ... 84
6.3.3 Projektumfang ... 84
6.3.4 Abhängigkeiten ... 85
6.3.5 Glücklose Projekthistorie ... 86
6.3.6 Vielzahl externer Auftragnehmer ... 87

6.3.7 Projektrisiko-Checkliste ... 88
6.3.8 Projektrisikoindikatoren ... 90
6.4 Geschäftsprozesse ... 94
6.4.1 Fehlendes Verständnis der vorhandenen Geschäftsprozesse ... 94
6.4.2 Auswirkungen auf zukünftige Geschäftsprozesse ... 95
6.4.3 Projektrisiko-Checkliste ... 95
6.4.4 Projektrisikoindikatoren ... 96
6.5 Anwender ... 97
6.5.1 Starre Organisationskultur ... 98
6.5.2 Mangelnde Zielübereinstimmung ... 98
6.5.3 Projektrisiko-Checkliste ... 99
6.5.4 Projektrisikoindikatoren ... 100
6.6 Technologie ... 101
6.6.1 Innovative bzw. neue Technologie ... 101
6.6.2 Komplexität des IT-Systems ... 102
6.6.3 Komplexität der Systemimplementation ... 103
6.6.4 Projektrisiko-Checkliste ... 103
6.6.5 Projektrisikoindikatoren ... 104
6.7 Daten ... 106
6.7.1 Fehlende Informationsarchitektur ... 108
6.7.2 Unzureichend dokumentierte Datenspeicher ... 108
6.7.3 Mangelnde Datenqualität ... 109
6.7.4 Projektrisiko-Checkliste ... 110
6.7.5 Projektrisikoindikatoren ... 111

7 Projektkontrollen aufnehmen und beurteilen 113

7.1 Vorgehensweise ... 113
7.1.1 Projektkontrollen aufnehmen ... 114
7.1.2 Projektkontrollen beurteilen ... 114
7.2 Geschäftliche Ausrichtung ... 116
7.2.1 Übereinstimmung mit den Geschäftszielen ... 116
7.2.2 Management des Projektportfolios ... 117
7.2.3 Definierte Projektziele ... 118
7.2.4 Umfassende Projektspezifikation ... 119
7.2.5 Projektrisikomanagement ... 122
7.2.6 Genehmigtes Projektbudget ... 123
7.2.7 Projektkontroll-Checkliste ... 123
7.2.8 Projektkontrollindikatoren ... 124
7.3 Projektmanagement ... 125
7.3.1 Bewährter Projektleitfaden ... 126
7.3.2 Dokumentierte Projektvereinbarung ... 126
7.3.3 Realistische Aufgaben- und Aufwandsplanung ... 128
7.3.4 Umfassende Projektplanung ... 129

7.3.5 Angemessene Projektorganisation ... 132
7.3.6 Projektüberwachung und -steuerung ... 135
7.3.7 Teammanagement ... 137
7.3.8 Kommunikationsmanagement ... 139
7.3.9 Auswahl und Management der Lieferanten ... 140
7.3.10 Problem und Change Management ... 142
7.3.11 Qualitätsmanagement ... 144
7.3.12 Geplanter Projektabschluss ... 145
7.3.13 Projektkontroll-Checkliste ... 146
7.3.14 Projektkontrollindikatoren ... 147
7.4 Geschäftsprozesse ... 150
7.4.1 Dokumentierte Ist-Prozesse ... 150
7.4.2 Dokumentierte Soll-Prozesse ... 151
7.4.3 Ordnungsmäßigkeit der Prozesse ... 151
7.4.4 Test der Prozesse ... 152
7.4.5 Projektkontroll-Checkliste ... 153
7.4.6 Projektkontrollindikatoren ... 154
7.5 Anwender ... 155
7.5.1 Berücksichtigung organisatorischer Veränderungen ... 155
7.5.2 Schulungsplanung ... 156
7.5.3 Professionelle Schulungsdurchführung ... 157
7.5.4 Projektkontroll-Checkliste ... 157
7.5.5 Projektkontrollindikatoren ... 158
7.6 Technologie ... 158
7.6.1 Bewährtes Vorgehensmodell ... 159
7.6.2 Geeignete Entwicklungsumgebung ... 160
7.6.3 Qualität des DV-Konzeptes ... 161
7.6.4 Qualität der Realisierung ... 162
7.6.5 Teststrategie und -planung ... 163
7.6.6 Systematische Testdurchführung ... 166
7.6.7 Testmanagement ... 168
7.6.8 Konfigurationsmanagement ... 171
7.6.9 Aussagekräftige Dokumentation ... 172
7.6.10 Ordnungsgemäße Inbetriebnahme ... 174
7.6.11 Projektkontroll-Checkliste ... 175
7.6.12 Projektkontrollindikatoren ... 176
7.7 Daten ... 178
7.7.1 Definierte Datenanforderungen ... 178
7.7.2 Umfassende Datenqualitätskontrollen ... 179
7.7.3 Planung der Datenbereitstellung ... 180
7.7.4 Test der Datenübernahme ... 180
7.7.5 Ordnungsgemäße Datenübernahme ... 181
7.7.6 Projektkontroll-Checkliste ... 183

7.7.7 Projektkontrollindikatoren ... 183

8 Risikoanalyse und -priorisierung 185

8.1 Projektrisiko- und -kontrollbereiche ... 185

8.2 Projektrisiken und Projektkontrollen ... 186

9 Risikobehandlungsmaßnahmen ergreifen 190

9.1 Maßnahmenauswahl ... 190

9.2 Maßnahmen zur Risikovermeidung ... 192

9.3 Maßnahmen zur Risikoverminderung ... 192

9.4 Maßnahmen zur Risikobegrenzung ... 195

9.5 Maßnahmen zur Risikoverlagerung ... 196

9.6 Maßnahmen zur Risikoakzeptanz ... 196

10 Projektrisiken überwachen 198

11 Übersicht Projektrisikofaktoren/ Projektkontrollziele 201

Literaturverzeichnis 203

Index 210

1 Vorwort

1.1 Vorwort zur 2. komplett neubearbeiteten Auflage

„Die Verantwortung für das Risikomanagement fällt jeweils der Partei zu, die den Preis für die ignorierten Risiken zahlt." [DeLi03]

Meine Vorhersage, dass das Thema Risikomanagement in IT-Projekten eines der zentralen Themen des nächsten Jahrzehnts beim Management und bei der Organisation von IT-Projekten werden wird, ist bereits teilweise in Erfüllung gegangen. Zahlreiche Seminaranbieter haben das Thema in ihre Programme aufgenommen, die Gesellschaft für Projektmanagement hat eine eigene Expertentagung zu diesem Themenkomplex durchgeführt und dieses Thema zum Schwerpunkt der Ausgabe 2/2003 von „Projektmanagement aktuell" werden lassen und letztendlich ist auch diese 2. Auflage eine Bestätigung dieses Trends. Diese Entwicklung freut mich natürlich. Gleichwohl besteht die Gefahr, dass so manche dieses Thema nun aufgreifen ohne es inhaltlich durchdrungen zu haben und damit dem Thema mehr schaden als nutzen.

Dieser Gefahr will ich durch die Neubearbeitung der 2. Auflage meines Buches entgegenwirken. Ich habe versucht, die Anregungen der Leser und Kritiker durch die sprachliche und grafische Überarbeitung aller Kapitel nachzukommen. Gleichzeitig wurden Angaben wo notwendig aktualisiert und einzelne Prozessschritte ausführlicher und klarer dargestellt.

Aus aktuellem Anlass habe ich insbesondere dem Thema Project Governance als wichtigen Bestandteil der Corporate bzw. IT-Governance mehr Raum eingeräumt. Eine Studie bei 100 ausgewählten IT-Verantwortlichen von Schweizer Unternehmen hat ermittelt, das die IT-Projektkosten pro Mitarbeiter fast genauso hoch sind wie die IT-Betriebskosten pro PC-Arbeitsplatz. Bezogen auf die Mitarbeiterzahl in den untersuchten Unternehmen wurden im Schnitt pro 1.000 Mitarbeiter 33 Projekte durchgeführt. Überragende Bedeutung hat dabei das Projektgeschäft in der Banken- und Versicherungsbranche: Dort wurden pro 1.000 Mitarbeiter durchschnittlich 75 Projekte durchgeführt und damit rund CHF 32.000 für IT-Projekte pro Mitarbeiter ausgegeben [ITKOST02]. Dies allein sollte bereits Beleg genug sein, warum Corporate bzw. IT-Governance auch Project Governance, also die aus Managementsicht notwendigen Kontrollen und Maßnahmen, um einen erfolgreichen Projektverlauf sicherzustellen, umfassen sollte.

Nicht erst seit der Aktualität des Themas Corporate Governance sollte das Management die regelmäßige Durchführung einer unabhängigen Risikoanalyse für jedes bedeutende Projekt verbindlich anweisen. Schließlich ist der Träger des Gesamtprojektrisikos und damit auch der meisten der vom Risikomanagement identifizierten Projektrisiken der Auftraggeber und damit das Management. Das Management würde in dieser Position grob fahrlässig handeln, wenn es inzwischen marktübliche Verfahren zur Früherkennung von Projektrisiken nicht einsetzen würde.

Weiterhin habe ich auch eine Webseite eingerichtet, die sich übergreifend mit dem Management von operativen Risiken, insbesondere aber dem Management von IT-Risiken und Projektrisiken, beschäftigt. Sie erreichen diese Webseite unter http://www.risikomanagement-in-it-projekten.de oder unter http://www.markus-gaulke.de.

Frankfurt am Main

Markus Gaulke, markusgaulke@kpmg.com

1.2 Vorwort zur 1. Auflage

„Managen Sie Projekte, indem Sie ihre Risiken managen“ (aus dem Tagebuch von Mr. Tompkins in [DeM98])

Ohne Informationstechnologie (IT) sind heutzutage auch traditionelle Branchen nicht mehr lebensfähig. Bei der Deutschen Bank AG repräsentieren die IT-Mitarbeiter bereits annähernd 30 % der Belegschaft [Frei01]. Entsprechend stellen die mit der Informationstechnologie verbundenen Risiken inzwischen einen bedeutenden Anteil der operativen Risiken in den Unternehmen dar. Auch der Gesetzgeber und die Aufsichtsbehörden haben die generelle Bedeutung des Managements von IT-Risiken im Rahmen der operativen Risiken erkannt und den Unternehmen teilweise bereits verbindliche Rahmenbedingungen vorgegeben.

Gleichzeitig ist die Informationstechnologie zum „Enabler“ für eine bessere Positionierung der Unternehmen im Wettbewerb geworden. Bei der DaimlerChrysler AG werden beispielsweise softwarebasierte Funktionen als Verkaufsfaktor und Innovationsfaktor der Zukunft gesehen [Gant01]. Diese Entwicklungen sorgen zusammen mit einer erhöhten Dynamik der Märkte und neuen Technologien weltweit für einen steigenden Bedarf an IT-Projekten. Allein die amerikanischen Unternehmen führen jedes Jahr rund 200.000 IT-Projekte durch und investieren dabei 275 Milliarden Dollar [SM1299].

Die erfolgreiche Abwicklung von IT-Projekten hat für die Wettbewerbsfähigkeit der Unternehmen eine strategische Bedeutung erlangt. Ein erfolgreiches Unternehmen muss in der Lage sein, IT-Projekte professionell durchzuführen, um neue Produkte und Dienstleistungen in hoher Qualität zeit- und kostengerecht am Markt einführen zu können.

Projektfehlläufer würden dazu führen, dass Unternehmen ihre Geschäftsstrategie nicht umsetzen und in der Folge ihre Geschäftsziele nicht oder nur teilweise erreichen können.

Der zunehmenden Bedeutung der IT-Projekte steht aber entgegen, dass ein Drittel aller IT-Projekte scheitert und fast die Hälfte aller IT-Projekte den geplanten Zeitrahmen oder das veranschlagte Budget substantiell überzieht [SM1299]. Die Kosten für Projektfehlläufer beliefen sich nach Schätzungen der Standish Group 1998 allein in den USA auf rund 75 Milliarden US-Dollar. Aus diesem Dilemma kann ein systematisches Risikomanagement helfen, durch das Fehlentwicklungen in IT-Projekten rechtzeitig und mit geringem Aufwand erkannt und unter Kontrolle gebracht werden können.

Derzeit hat Risikomanagement in IT-Projekten in der Unternehmenspraxis jedoch lediglich eine untergeordnete Bedeutung. Die Vorstellungen von Risikomanagement in IT-Projekten reichen vom Ausfüllen einfacher Risikolisten bis zur Erstellung von umfangreichen Risikokatalogen mit Risikoblättern für jedes Einzelrisiko. In der Anwendung werden zudem häufig Risikoursachen und Risikoauswirkungen verwechselt, Risiken und Kontrollen vermischt oder notwendige Kennzahlen zur Risikoüberwachung vernachlässigt. Ein solches Risikomanagement wird dann schnell als lästige Pflichtübung wahrgenommen.

Das vorliegende Buch hat zum Ziel, eine praxiserprobte und handhabbare Methode mit allen benötigten Hilfsmitteln für das Risikomanagement in IT-Projekten vorzustellen. Die Methode ist dabei so flexibel aufgebaut, dass jederzeit Anpassungen und Erweiterungen möglich sind oder auch nur einzelne Elemente der Methode (z.B. die Risikoindikatoren) in ein vorhandenes unternehmenseigenes Risikomanagementsystem übernommen werden können. Checklisten mit Leitfragen am Ende jedes Projektrisiko- und -kontrollbereiches erleichtern die Arbeit mit der Methode und können bei Bedarf ebenfalls unternehmensspezifisch (z.B. in Richtung einer quantitativen Risikobewertung) erweitert werden.

Risikomanagement in IT-Projekten wird eines der zentralen Themen des nächsten Jahrzehnts beim Management und bei der Organisation von IT-Projekten werden. Auch eine Weiterentwicklung der bestehenden gesetzlichen und aufsichtlichen Rahmenbedingungen für das Management der operativen Risiken ist in diesem Sinne zu erwarten. Das Buch richtet sich daher grundsätzlich an alle Leser mit Interesse an den Themen Projektmanagement oder Risikomanagement. In der Unternehmens- und Beratungspraxis können vor allem Projektverantwortliche und Projektleiter sowie Risiko- und Qualitätsmanager von den dargestellten Inhalten profitieren. Gleichzeitig soll dieses Buch aber auch die Diskussion über die Bedeutung des Risikomanagements für das erfolgreiche Management von IT-Projekten anregen und bereichern.

Zu Beginn des Buches werden die notwendigen Begriffe sowie die gesetzlichen und verschiedene normative Anforderungen erläutert. Anschließend werden anhand von Studien und anderen Quellen die Ursachen für Projektfehlläufer sowie die Erfolgsfaktoren für IT-Projekte diskutiert. Die folgenden Kapitel widmen sich dann der Erläuterung der vorgestellten Methode für ein umfassendes Risikomanagement in IT-Projekten, die insbesondere durch die Integration von Indikatoren, Projektsteuerungs- und

-kontrollverfahren und Risikobehandlungsmaßnahmen auch viele praktische Anregungen für Verbesserung des Managements von IT-Projekten enthält.

Frankfurt am Main

Markus Gaulke, markusgaulke@kpmg.com

2 Einführung

„Risk management means dealing with a concern before it becomes a crisis.“ (Karl E. Wiegers in [Wie98])

Das folgende Kapitel soll mit einigen grundlegenden Begriffen vertraut machen und diese Begriffe insbesondere spezifisch für das Thema dieses Buches in den richtigen Kontext setzen.

2.1 Grundlegende Begriffe

An dieser Stelle werden einleitend die Begriffe „Projekt“, „Risiko“, „Projektrisiko“ und „Risikomanagement“ kurz erörtert. Die Erörterung soll einerseits einem gemeinsamen Verständnis der verwendeten Begriffe dienen, da in der Projekt- und Risikomanagement-literatur teilweise unterschiedliche Definitionen angewandt werden. Andererseits werden diese Begriffe bereits im Sinne der in den nachfolgenden Kapiteln beschriebenen Methodik für eine Risikomanagement in IT-Projekten interpretiert.

2.1.1 Projekt

Nach DIN 69901 ist ein Projekt ein „Vorhaben, das im wesentlichen durch Einmaligkeit der Bedingungen in ihrer Gesamtheit gekennzeichnet ist, wie z.B. Zielvorgabe, zeitliche, finanzielle, personelle und andere Begrenzungen, Abgrenzungen gegenüber anderen Vorhaben oder eine projektspezifische Organisation.“

In der Praxis wird ein Projekt auch als ein Vorhaben mit den folgenden Merkmalen definiert [GAB88] [STE98]:

- Bedeutung des Projektergebnisses

Das angestrebte Projektergebnis sollte für den Auftraggeber bedeutsam sein. In Unternehmen sollte das Projektergebnis beispielsweise die Erfüllung der Geschäftstrategie oder die Umsetzung konkreter Geschäftsziele maßgeblich unterstützen.

- Einmaligkeit der Projektaufgabe

Die Projektaufgabe sollte einmalig und keine wiederkehrende Tätigkeit sein.

- zeitliche Befristung

Jedes Projekt sollte einen definierten Endtermin besitzen.

- Umfang und Komplexität

Ein Projekt sollte hinsichtlich des zeitlichen und personellen Aufwandes zur Aufgabendurchführung sowie des Schwierigkeitsgrades der Aufgabenstellung bedeutend sein. Der Umfang und die Komplexität des Vorhabens erfordern in der Regel ein gesondertes Management.

- Beteiligung mehrerer Organisationseinheiten

Ein Projekt beinhaltet in der Regel übergreifende Aufgabenstellungen und erfordert die Zusammenarbeit von verschiedenen Fachbereichen. Die Beteiligung mehrerer organisatorischer Einheiten macht häufig eine spezielle Projektorganisation notwendig.

- Innovation

Ein Projekt umfasst in der Regel Aufgabenstellungen, die für die Beteiligten neu sind bzw. in der Vergangenheit in dieser Form noch nicht bewältigt werden mussten.

- Risikobehaftung

Die oben genannten Merkmale, insbesondere die Einmaligkeit, die Innovation sowie der Umfang und die Komplexität der Aufgabe bedingen, dass ein Projektvorhaben grundsätzlich risikobehaftet ist. Risikobehaftung kann damit als ein weiteres Merkmal eines Projektes angesehen werden.

Unter einem IT-Projekt wird im folgenden ein Vorhaben mit den dargestellten Projektmerkmalen verstanden, bei dem zusätzlich der Erfolg des Projektes maßgeblich von der Auswahl, Analyse, Entwicklung, Wartung, Weiterentwicklung oder Einführung mindestens eines Informations- oder Kommunikationssystems abhängt. Entsprechend sind die meisten Projekte in den Unternehmen heutzutage IT-Projekte, da beispielsweise auch Projekte mit dem Ziel der Umstrukturierung oder der Geschäftsprozessoptimierung ohne Änderungen oder Ergänzungen an den IT-Systemen (z.B. an Controlling- oder Workflow-Systemen) kaum vorstellbar sind.

Das Spektrum der möglichen IT-Projekte ist demnach riesig. Erstmal können das oder die betroffene(n) Informations- oder Kommunikationssysteme ganz unterschiedlicher Art sein: Projekte mit kaufmännische Anwendungen unterscheiden sich beispielweise erheblich von Projekten mit technischen Anwendungen oder systemnahen Applikationen.

Auch nach der Art des Projektes unterscheiden sich IT-Projekte voneinander, je nachdem ob eine Neuentwicklung erfolgen soll, oder nur ein Re-Design oder eine Weiterentwicklung eines Systems Projektinhalt ist. Eine Neuentwicklung lässt sich nach der Anzahl der zukünftigen Anwendungsorganisationen wiederum in Individualsoftware und Standardsoftware weiter differenzieren. Im kaufmännischen Bereich ist heutzutage die Auswahl und Anpassung sogenannter „COTS-Software“ ein typisches IT-Projekt. COTS steht für „Commercial Of The Shelf“, also für betriebswirtschaftliche Standardsoftware (z.B.

SAP R/3), die auf Basis der Anforderungen des Unternehmens hin ausgewählt wird und auf die Bedürfnisse noch mehr oder weniger angepasst werden muss.

Im Zuge der zunehmenden Zusammenschlüsse oder Kooperationen von Unternehmen stehen darüber hinaus vielfach Integrationsprojekte an, bei denen im Rahmen von IT-Projekten die unterschiedlichsten IT-Systeme und die damit zusammenhängenden Geschäftsprozesse vereinheitlicht und integriert werden müssen.

Im Zentrum der nachfolgenden Betrachtungen stehen in erster Linie Projekte mit kaufmännischen Anwendungen in allen genannten Projektarten. Auf die Besonderheiten der einzelnen Projektarten kann die nachfolgend vorgestellte Methode für das Projektrisikomanagement über die Gewichtung der einzelnen Projektrisikofaktoren und Projektkontrollziele leicht angepasst werden. Aber auch für Projekte mit dem Ziel, rein technische Anwendungen zu erstellen, ist die Methode prinzipiell anwendbar, auch wenn dann einzelne Projektrisikofaktoren und Projektkontrollziele (vor allem in den Projektbereichen „Geschäftsprozesse“, „Anwender“ und „Daten“) auf ihre Relevanz überprüft werden müssen. Die zentralen Projektbereiche „geschäftliche Ausrichtung“, „Projektmanagement“ und „Technologie“ sind beim Risikomanagement in IT-Projekten jedoch allgemeingültig.

2.1.2 Risiko

Unter Risiko wird im betrieblichen Bereich allgemein die Gefahr verstanden, dass Ereignisse oder Handlungen ein Unternehmen daran hindern, seine Ziele zu erreichen bzw. seine Strategien erfolgreich umzusetzen [KPMG00]. Andere Quellen definieren Risiko allgemein als „Möglichkeit ungünstiger künftiger Entwicklungen“ [WPH00] oder als „Gefahr, die den Prozess der Zielsetzung und Zielereichung begleiten und ihn negativ beeinflussen können“ [GAB88].

Eine weitergehende Definition des Begriffes „Risiko“ [Sch97] beschreibt Risiko als ein „Ereignis, von dem nicht sicher bekannt ist, ob es eintreten und/ oder in welcher genauen Höhe es einen Schaden verursachen wird.“ Ein Ereignis, dass mit Sicherheit eintreten wird, stellt demnach ein Problem und kein Risiko dar.

Die obige Definition von Risiko enthält sowohl den Bestandteil der Unsicherheit über ein Ereignis als auch den Bestandteil der negativen Auswirkung eines Ereignisses. Das Risiko kann mathematisch entsprechend als Funktion aus den berechenbaren Größen Wahrscheinlichkeit und Schadenshöhe betrachtet werden.

In der Statistik ergibt sich die Wahrscheinlichkeit W(A) als Größe, der sich die relative Häufigkeit eines Ereignisses A bei unbeschränktem Umfang der Versuchsserie nähert [Puh89]. Aus dieser Definition wird auch das Kernproblem der Wahrscheinlichkeits-berechnung im Rahmen der Risikobetrachtung bei IT-Projekten erkennbar. Die zuverlässige Wahrscheinlichkeitsberechnung bedarf einer umfangreichen Anzahl von Beobachtungen, die in der Regel nur schwierig durchzuführen sein werden. Einen Ausweg aus diesem Dilemma bietet die subjektive Auffassung der Wahrscheinlichkeit. Dabei werden

Wahrscheinlichkeitsaussagen als subjektiver Überzeugtheitsgrad oder anschaulicher als Wettbereitschaft einer (sachkundigen) Person im Hinblick auf das Eintreten eines Ereignisses betrachtet.

Die Schadenskomponente beim Risiko wird gewöhnlich in Geldeinheiten gemessen. Der Schaden im Falle von gescheiterten IT-Projekten betrifft in Unternehmen aber auch nicht-monetäre Unternehmensziele, wie die Reputation oder die Produktqualität, deren Verschlechterung sich erst mit der Zeit auf die monetären Unternehmensziele auswirkt. Diese nicht-finanziellen Dimensionen der Schadensauswirkung macht die Quantifizierung der Schadenshöhe bei IT-Projekten in der Praxis ebenfalls sehr schwierig.

2.1.3 Projektrisiko

Das spezielle Risiko bei Projekten ist in verschiedenen Publikationen ebenfalls definiert worden. Madauss [Mad00] definiert Risiko im Projektzusammenhang als die „Unwägbarkeit des technischen und/ oder wirtschaftlichen Projekterfolges."

In der DIN 62198 wird Projektrisiko als die „Kombination aus der Eintrittswahrscheinlichkeit eines bestimmten Ereignisses und seinen Folgen für die Projektziele" beschrieben. Projektrisiken werden sowohl im Projekt als auch im Umfeld des Projektes gesehen. Als Beispiele für Risikofaktoren, die ein Projekt beeinträchtigen können, sind aufgeführt:

- Umwelt
- Markt
- Gesellschaft
- Finanzen
- Zuverlässigkeit
- Wirtschaft
- Mensch
- Technik
- Recht

Das Project Management Institute (PMI) definiert ein Projektrisiko als „ein unsicheres Ereignis oder eine Bedingung, dessen/ deren Eintreten eine positive oder negative Auswirkung auf ein Projektziel hat" [PMBOK03]. Damit umfasst die Definition sowohl Risiken, die eine Gefährdung der Projektziele bedeuten als auch Chancen, die sich in einer Übererfüllung der Projektziele darstellen können. Weiterhin werden Ereignisrisiken und Bedingungsrisiken unterschieden: Ein Ereignisrisiko ist beispielsweise ein späte Erteilung einer Genehmigungen; ein Bedingungsrisiko enthält dagegen Aspekte in der Projektumgebung, wie schlechte Projektmanagementpraktiken oder die Abhängigkeit von externen Teilnehmern.

Jedes Projektrisiko hat eine Ursache und, wenn das Risiko eintritt, eine Auswirkung. Die Auswirkungen betreffen die Projektkosten, den Zeitplan oder die Qualität der

3 Notwendigkeit für ein Risikomanagement bei IT-Projekten

„Der Vorstand hat nach § 91 Abs. 2 AktG ein angemessenes Risikomanagementsystem einzurichten. Aufgrund der besonderen wirtschaftlichen Bedeutung von Großprojekten für die Unternehmung sollte grundsätzlich auch innerhalb bedeutender Projekte ein entsprechendes Subsystem eingerichtet werden." [Bet0602]

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

- 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. reine Vertriebsbanken) ermöglichen
- Informationstechnologie als „Enabler" für eine bessere Positionierung des Unternehmens im Wettbewerb
- Steigende Anforderungen des Gesetzgebers und der Aufsichtsbehörden (z.B. die Mindestanforderungen an das Betrieben von Handels- und Kreditgeschäften, das KonTraG, Basel II)

Dazu kommen die besonderen inhärenten Risiken bei IT-Projekten im Vergleich zu anderen Projekten, wie beispielsweise Konstruktionsprojekten. Software ist einerseits ein immaterielles Gut, dessen Fertigstellungsgrad und Qualität durch die menschlichen Sinne nicht wahrgenommen werden kann und andererseits findet Softwareentwicklung oftmals in einem äußerst komplexen und dynamischen technologischen Umfeld statt. Diese beiden wesentlichen Besonderheiten von IT-Projekten haben Konsequenzen:

- Aufwandsschätzungen sind schwierig zu erstellen

Bedingt durch den technologischen Wandel fehlen häufig Erfahrungswerte und die vorhandenen Schätzmethoden müssen immer wieder auf die spezifischen Erfordernisse und Rahmenbedingungen des jeweiligen IT-Projektes angepasst werden.

- Entwicklungsfortschritte sind schwer messbar

Während der Softwareentwicklung lässt sich der Fertigstellungsgrad der Software nur schwer zuverlässig bestimmen. Ob die Software den funktionalen und systemseitigen Anforderungen entspricht, lässt sich oftmals erst in der Testphase ermitteln.

- Hohe Einarbeitungszeiten der Projektmitglieder

Während sich Verzögerungen bei einem Bauvorhaben durch eine Erhöhung der Anzahl Maurer vielleicht kompensieren lassen, ist dies aufgrund der Einarbeitungszeit in das technologische Umfeld bei IT-Projekten nicht kurzfristig möglich.

- Anforderungen ändern sich während der Projektlaufzeit

Neben geschäftlichen und gesetzlichen Änderungen der Rahmenbedingungen führt die Abstraktheit der Software auf der Anwenderseite regelmäßig zu Änderungen der Anforderungen während der Projektlaufzeit. Dazu kommen der technologische Fortschritt und die gesammelten Erfahrungen während der Softwareentwicklung, die wiederum in Projektänderungen münden können.

Auch durch den zunehmenden Einsatz von Standardsoftware wird das Risikomanagement in IT-Projekten nicht überflüssig. Die Auswahl und Implementation von Standardsoftware erfordert ebenso die klassischen Projektphasen Fachkonzeption, DV-Konzeption (teilweise), Test (teilweise) und Einführung wie die klassische Eigenentwicklung. Allein die Realisierungsphase wird durch eine Customizing-Phase ersetzt, bei der die Standardsoftware entsprechend den Anforderungen des Unternehmens parametrisiert wird. Das Customizing stellt hohe Anforderungen an das Projektmanagement, insbesondere erfordert es als fachlich-technische Aufgabenstellung sowohl qualifizierte IT-Mitarbeiter als auch die intensive Beteiligung der Fachbereiche.

Besondere Beachtung verdient beim Einsatz von Standardsoftware auch die Ausgestaltung der Geschäftprozesse, da in der Software Annahmen über betriebliche Strukturen und Abläufe enthalten sind und die vorhandenen Geschäftprozesse von der Standardsoftware in der Regel nicht unterstützt werden. Auch die Projektrisiko und -kontrollbereiche „Geschäftliche Ausrichtung“, „Anwender“ und „Daten“ spielen bei der Einführung von Standardsoftware eine wichtige Rolle.

Die Notwendigkeit für ein Risikomanagement bei IT-Projekten wird in diesem Kapitel aus gesetzlicher und aufsichtsrechtlicher Sicht sowie aus der Sicht von verschiedenen, anerkannten Leitfäden und Standards diskutiert und abschließend exemplarisch durch einige Studien untermauert. Dabei wird deutlich, dass – trotz fehlender gesetzlicher bzw. aufsichtsrechtlicher Konkretisierung – Risikomanagement ein fester Bestandteil eines jeden größeren IT-Projektes sein sollte.

4 Ursachen für Projektfehlläufer und Erfolgsfaktoren

„Analysis of software project failures in the last decades indicates that most of the problems can be traced back from one or more project high level risk areas." [DriveSPI97]

Im folgenden sind einige der zahlreichen Studien zu den Themengebieten IT-Projektmanagement und Softwareentwicklung aufgeführt. Zusätzlich werden auch ausgewählte „Expertenmeinungen" angeführt, die nicht immer auf umfangreichen Studien beruhen, aber auch sehr wertvolle Erkenntnisse liefern. Aus den Ursachen für Projektfehlläufer ergeben sich in der Regel auch die Erfolgsfaktoren. Daher werden die Erfolgsfaktoren – soweit untersucht – in den einzelnen Abschnitten direkt mitbehandelt.

Die in den verschiedenen Quellen genannten Ursachen für Projektfehlläufer haben teilweise einen hohen Überdeckungsgrad und stellen damit typische Projektrisiken dar, die in keiner Methode zur Unterstützung der Identifikation von Projektrisiken fehlen sollten.

4.1 Studien

Die nachfolgend zitierten Studien (ohne Wertung und in chronologischer Reihenfolge) sind von verschiedenen Organisationen in unterschiedlichen Ländern mit diversen Methoden durchgeführt worden. Obwohl die Ursachen für das Scheitern von IT-Projekten vielfältig sind, ergibt sich aus der Zusammenschau der Studien ein relativ einheitliches Bild der wesentlichen Projektrisiken. Insbesondere die Aspekte unzureichende Anforderungen, mangelnde Planung und fehlende Benutzereinbindung / Managementunterstützung tauchen in den Studien immer wieder auf.

4.1.1 KPMG-Studie: "IT Runaway Systems"

KPMG Management Consulting hat 1994 eine Telefonumfrage bei über 1.200 britischen Unternehmen aus verschiedensten Branchen durchführen lassen. Die Befragten wurden im Interview anhand ihrer Erfahrung mit IT-Projekten, der Größe der IT-Projekte in ihren Unternehmen und ihrer Zugehörigkeit weiter selektiert, um nur repräsentative Aussagen in die Studie aufzunehmen.

Die Umfrage basierte schließlich auf 120 kompletten Interviews. Von diesen 120 Befragten hatten 46 (38%) keine Projektfehlläufer angegeben, so dass die nachfolgenden Angaben zu den Ursachen von Projektfehlläufern auf den Aussagen der 74 (62%) verbleibenden Befragten basieren [KPMG94].

Als Ursachen, die zum Scheitern des Projektes führten, wurden am häufigsten angeführt:

Tab. 4.1 *Ursachen für Projektfehlläufer lt. KPMG-Studie: „IT Runaway Systems"*

Gründe für Projektfehlläufer	Anteil
Projektziele nicht ausreichend definiert	51 %
Schlechte Planung und Schätzung	49 %
Anwendung neuer Technologien	45 %
Unzureichende Projektmanagementmethoden	42 %
Mangel erfahrener Mitarbeiter im Projektteam	42 %
Schlechte Leistung der Lieferanten von Hardware / Software	42 %
Falsche Besetzung der Position des Projektleiters	35 %
Unzureichende Softwareentwicklungsmethoden	35 %
Überehrgeizige Projektziele	34 %
Falsche Besetzung des Projektteams	34 %
Schlechte Kommunikation zwischen Projektmitgliedern	32 %
Fehlende Kenntnis über Projektprobleme beim Management	30 %

Die Befragten gaben darüber hinaus folgende Ratschläge, um in Zukunft Projektfehlläufer zu vermeiden:

- Externe Lieferanten nach den Kriterien Zuverlässigkeit und Know-how genauer aussuchen
- Internes IT-Projektteam und Benutzer besser einweisen
- Anwendung von Reviews und Risikoanalyse bei komplexen Projekten in den einzelnen Projektphasen
- Enge Zeitplanung und –kontrolle entlang des kritischen Pfades
- Einbindung des Managements auf angemessener Ebene
- Beurteilung der Technologie im Vorfeld des Projektes
- Genaue Zeit- und Kostenplanung
- Alternativen im Falle von Änderungen der politischen oder strategischen Ausrichtung bedenken

5 Kurzdarstellung der Vorgehensweise

„Verschwendung, Verschwendung, Verschwendung. Verschwendung und Risiko gehen meiner Meinung nach Hand in Hand. Der wirklich vergeudete Anteil der Projektarbeit ist immer die direkte Folge eines auftretenden Risikos. So entstehen die Vergeudungen, die Sie wirklich zurückwerfen. Deshalb würde ich mich in aller erster Linie für das Risikomanagement stark machen. Ich würde jedes Projekt managen, indem ich die Risiken manage, mit denen das Projekt konfrontiert ist. Software-Entwicklung ist ein riskantes Geschäft, und Management ist in dieser Branche vor allem und zuallererst eine Übung in Risikomanagement.“ (Dr. Rizzoli zu Mr. Tompkins in [DeM98])

Die in diesem Buch vorgestellte Vorgehensweise berücksichtigt sowohl in ihrer Methodik als auch in ihrem Inhalt zahlreiche praktische und theoretische Erkenntnisse aus verschiedenen Informationsquellen. Die wichtigste Informationenquelle ist meine eigene Erfahrung als Projektmanager und Projektreviewer sowie die Erfahrung vieler Kollegen im internationalen KPMG-Verbund aus Standortbestimmungen und projektbegleitenden sowie projektnachgelagerten Reviews von IT-Projekten unterschiedlichster Größe. Als weitere Informationsquellen dienten sowohl diverse Studien über Erfolgsfaktoren für das Gelingen und über Gründe für das Scheitern von IT-Projekten (s. insbesondere Kapitel 4) als auch die international verfügbare Literatur zum Thema Risikomanagement in IT-Projekten (s. insbesondere Kapitel 3).

5.1 Methodik

Die nachfolgend vorgestellte Vorgehensweise für ein Risikomanagement in IT-Projekten hat als primäres Ziel, Projektrisiken, deren Auswirkungen erst später im Projektverlauf auftreten, frühzeitig zu erkennen, um geeignete und wirksame Projektsteuerungsmaßnahmen ergreifen zu können. Zu diesem Zweck beruht die Vorgehensweise methodisch auf einem Risikomanagement-Kreislauf, der mit der Risikoerkennung beginnt. Der Risikomanagement-Kreislauf soll sicherstellen, dass die Methode kontinuierlich und einheitlich angewandt werden kann. Der für das Risikomanagement von IT-Projekten verwendete Kreislauf besteht aus den folgenden fünf Schritten:

1. Projektrisiken erkennen und beurteilen

6 Projektrisiken erkennen und beurteilen

"Only those risks that have been identified can be managed." [CCTA00]

Projektrisiken sind mögliche Bedrohungen für den Erfolg eines Projektes. Diese Projektrisiken können bekannt, unbewusst oder unvorhersehbar sein. Bekannte Projektrisiken sind Risiken, die mindestens einem Projektbeteiligten bewusst sind. Unbewusste Projektrisiken sind solche, die den Projektbeteiligten auffallen, wenn sie die entsprechenden Anregungen, Hinweise oder Informationen erhalten. Die bekannten und unbewussten Risiken systematisch zu erfassen und zu beurteilen, ist das Ziel des ersten Schrittes der hier vorgestellten Methode für das Risikomanagement bei IT-Projekten. Unvorhersehbare Projektrisiken sind Risiken, die per Definition nicht erkannt werden können und unter die Rubrik allgemeines unternehmerisches Risiko fallen [SEI93].

6.1 Vorgehensweise

Herzstück eines effizienten Risikomanagements von IT-Projekten ist die systematische Sichtbarmachung und Beurteilung der inhärenten Projektrisiken. Inhärente Risiken sind Risiken, die in einem Prozess grundsätzlich existieren, d.h. bevor Kontrollen eingerichtet worden sind. Bei IT-Projekten hängen diese inhärenten Risiken u.a. von der Art des IT-Projektes, vom Industriezweig und dessen Marktumfeld, von der Struktur und Kultur des Unternehmens sowie von der eingesetzten Technologie ab.

6.1.1 Projektrisiken erkennen

„most project risks are usually known by project personnel" [SEI93]

Die systematische Identifikation der inhärenten Projektrisiken basiert bei der in diesem Buch vorgestellten Methode auf einem Risikokatalog, der die Erfahrungen aus vergangenen eigenen und fremden IT-Projekten zusammenfasst. Die Vorgabe des Risikokataloges soll dabei keinesfalls eine Beschränkung auf diese Risikofaktoren implizieren, sondern in erster Linie als Vollständigkeitskontrolle und Qualitätssicherung dienen.

7 Projektkontrollen aufnehmen und beurteilen

"Proper project implementation includes controls, policies and procedures, training, testing, contingency planning, and proper oversight of any outsourcing." [OCC983]

Bei der Aufnahme und Beurteilung der Projektkontrollen wird die Wirksamkeit der vorhandenen Projektsteuerungs- und -kontrollverfahren (im folgenden teilweise auch kurz „Projektkontrollverfahren" genannt) bzw. – je nach Analysetiefe - der konkreten Projektkontrollen ermittelt. Die Erfassung und Beurteilung der Projektkontrollen erfolgt im Rahmen der gleichen Projektbereichssystematik wie die Identifikation und Beurteilung der inhärenten Projektrisiken. Dadurch ermöglicht die Vorgehensweise, am Ende sowohl zu einer Bewertung der verbleibenden Projektrisiken auf der Ebene der Projektrisiko- und -kontrollbereiche zu gelangen als auch konkreten Projektrisiken entsprechende Projektkontrollen gegenüber zu stellen.

Die klare Trennung zwischen der Aufnahme und Beurteilung der Projektrisiken und Aufnahme und Beurteilung der Projektkontrollen ermöglicht insbesondere eine risikoorientierte Schwerpunktsetzung bei der Beurteilung der Projektsteuerungs- und -kontrollverfahren bzw. der Projektkontrollen in den als risikobehaftet identifizierten Projektbereichen und damit eine effiziente Vorgehensweise für das Projektrisikomanagement. Für Projektbereiche, in denen kein hohes inhärentes Risiko festgestellt wurde, kann die Aufnahme der Projektkontrollverfahren entweder komplett entfallen oder in vermindertem Umfang durchgeführt werden.

7.1 Vorgehensweise

Zur Beurteilung der Projektkontrollen müssen die vorhandenen und geplanten Projektsteuerungs- und -kontrollverfahren in den als kritisch definierten Projektbereichen aufgenommen und deren Angemessenheit und Effektivität beurteilt werden.

8 Risikoanalyse und -priorisierung

„You can never really control risks, only manage them.“ (Gregory Parker)

Die Risikoanalyse und –priorisierung findet bei IT-Projekten auf zwei Ebenen statt. Einerseits erfolgt eine Darstellung der Risikointensität und der Kontrollstärke auf Ebene der Projektrisiko- und -kontrollbereiche, die einen sehr guten Überblick über die allgemeine Risikosituation des IT-Projektes erlaubt. Andererseits muss eine Analyse und Priorisierung auf der Ebene der einzelnen Projektrisikofaktoren und Projektkontrollziele bzw. der konkreten Projekteinzelrisiken und -kontrollschwächen erfolgen, da erst auf dieser Ebene eine wirtschaftliche Maßnahmensteuerung und Risikoüberwachung ermöglicht.

8.1 Projektrisiko- und -kontrollbereiche

Auf Basis der bewerteten Projektrisikofaktoren und Projektkontrollziele wird das Restrisiko bzw. Netto-Risiko für jeden Projektrisiko- und -kontrollbereich ermittelt. Zur Darstellung der ermittelten Restrisiken bietet sich auf Ebene der Projektrisiko- und -kontrollbereiche eine Risiko-Kontroll-Matrix an. Diese Darstellung gibt die Einschätzung der Projektrisiken nach Beurteilung der implementierten Projektsteuerungs- und -kontrollverfahren wieder. Hierbei resultiert der Wert auf der Ordinate aus der Beurteilung der inhärenten Projektrisikofaktoren in den genannten Projektbereichen und der Wert auf der Abszisse aus der Beurteilung des Erreichungsgrades der Projektkontrollziele. Dabei ist in der Abbildung folgende Zuordnung der Projektrisiko- und -kontrollbereiche (PB) getroffen worden:

1. Geschäftliche Ausrichtung
2. Projektmanagement
3. Geschäftsprozesse
4. Anwender
5. Technologie
6. Daten

Abb. 8.1 *Risiko-Kontroll-Matrix auf Ebene der Projektrisiko- und -kontrollbereiche (PB)*

9 Risikobehandlungsmaßnahmen ergreifen

„If you do not actively attack the risks on your project, they will actively attack you." (Tom Gilb)

Auf Basis der analysierten und priorisierten Projektrisiken können in dieser Phase des Risikomanagementprozesses für IT-Projekte gezielt Projektsteuerungs- und -kontrollmaßnahmen zur weiteren Risikobehandlung festgelegt werden. Bei der Festlegung der Maßnahmen zur Risikobehandlung sollte sich an der klassischen Risikoreduktionstreppe [Gau00] orientiert werden, die aus den folgenden abgestuften Typen von Maßnahmen besteht:

- Risikovermeidung
- Risikoverminderung
- Risikobegrenzung
- Risikoverlagerung
- Risikoakzeptanz

Abb. 9.1 *Risikoreduktionstreppe*

Die Risikoreduktionstreppe verdeutlich die schrittweise Reduktion der erkannten Projektrisiken. Nicht erkannte Projektrisiken sind offensichtlich nicht Gegenstand der Behandlungsmaßnahmen. Die Dreiecke symbolisieren beispielhaft Maßnahmen zur Risikobehandlung. Am Ende der Risikotreppe steht die Risikoakzeptanz als bewusste Entscheidung der Projektverantwortlichen.

9.1 Maßnahmenauswahl

Die Entscheidung, welche Risikobehandlungsmaßnahmen aus der Vielzahl der Alternativen ergriffen werden sollen, obliegt den Projektverantwortlichen. In der Praxis sollte diese Entscheidung gemeinsam vom Management und dem Projektleiter getroffen werden.

10 Projektrisiken überwachen

"In summary, risk assessment is a tool that can yield excellent results at a low investment – but requires an unbiased, external mediator to establish the right mind-set as well as follow-through to be effective." [Mag01]

Projektrisiken überwachen bedeutet, die identifizierten Risiken laufend zu beobachten, neue und sich verändernde Risiken zu identifizieren sowie die Umsetzung und Wirksamkeit der geplanten Maßnahmen zu kontrollieren.

Im Sinne einer Funktionstrennung und der Umsetzung des „Vier-Augen-Prinzips" sollte die Überwachung der Projektrisiken in jedem Fall durch eine unabhängige Stelle erfolgen, die sowohl vom Projektleiter als auch von den IT- und Fachbereichen unabhängig ist [Gau01]. Hintergrund dieser Forderung ist u.a., dass die in das Projekt involvierten Personen sich häufig schnell daran gewöhnen, mit den Risiken zu leben anstatt diese konsequent zu managen [Mag01]. Auch DeMarco fordert einen neutralen Risikobeauftragten zu ernennen und diesen von der „Das-Schaffen-wir-Haltung" zu entbinden [DeM98].

Die Hauptaufgaben eines Projektrisikomanagers im engeren Sinne sind:

- Verfolgung der identifizierten Projektrisiken und geplanten Maßnahmen

Zur Verfolgung der identifizierten Projektrisiken und geplanten Maßnahmen sollte eine Risikoliste (sog. „Projektrisikoregister") angelegt werden, die alle identifizierten Risiken, die Einschätzung ihrer Auswirkungen sowie die beschlossenen Maßnahmen und Termine beschreibt. Das Projektrisikoregister sollte von Projektbeginn an geführt werden und stellt die Basis für die Risikoberichterstattung als auch für alle Risikobesprechungen dar. Für jedes Projektrisiko sollte ferner ein Risikoeigentümer (engl. Risk Owner) festgelegt werden, der für die Umsetzung beschlossenen Projektsteuerungs- und -kontrollmaßnahmen zum festgesetzten Termin und damit für die zeitgerechte Bewältigung des identifizierten Projektrisikos verantwortlich ist.

- Überwachung der Projektrisiken

Anhand von Frühwarnindikatoren können Projektrisiken permanent verfolgt werden. Anregungen für solche Risikoindikatoren sind am Ende der einzelnen Projektrisiko- und -kontrollbereiche für die dargestellten Projektrisikofaktoren und Projektkontrollziele aufgeführt (s. Kapitel 6 und 7). Veränderungen dieser Frühwarnindikatoren können auf Risiken hindeuten und müssen analysiert werden.

Index

ABC-Analyse 189

Abhängigkeiten 85, 127

Abnahmeprotokoll 171

Abnahmetest 130, 169, 173

Abstimmung 153, 181, 183, 186

Aktivitätenplan 61

Aktivsumme 191, 194

Altsysteme 44

Analogiemethode 128

Änderungskontrolle 60

Anforderungen 51, 53, 55, 57, 58, 62, 125, 195

Annahmen 127

Anwender 97, 156, 196

Arbeitsmittel 196

Arbeitspakete 196

Arbeitsumgebung 138

Association for Project Management 37

Attribut 109

Aufbewahrungsfrist 184

Aufgabenblöcke 149

Aufgabenplanung 128

Aufwand 80, 91, 178

Aufwandsschätzung 129

Balkendiagramme 131

Basel II 30

Benutzerdokumentation 174

Benutzereinbindung 51, 61

Benutzergruppen 92

Benutzerschnittstellen 62

Betriebskonzept 176

Betriebsverfassungsgesetz 98

BOOTSTRAP 34, 45

Bundesdatenschutzgesetz 77

Bundesministerium für Bildung und Forschung 54

Business Case 59

Capability Maturity Model 32, 58

Carnegie Mellon University 32, 42

Central Computer and Telecommunication Agency 43

Change Management 143

Change Requests 124, 150

CHAOS-Report 47, 51

Cleanroom Engineering 131

COBIT 39

Constructive Cost Model 128

Contingency Allowance 199

Controlling 15

Corporate Governance 21
Customizing 20
Daily Telegraph-Studie 53
Data Dictionary 120
Data Point 128
Daten 44, 107, 111, 179
Datenanforderungen 180
Datenbereinigung 181
Datenbestände 112
Datendarstellung 107
Datendefinition 107, 109
Datenlieferanten 112
Datenqualität 106, 109, 180, 185
Datenqualitätskontrollen 180
Datensätze 112, 185
Datensicherung 176
Datenspeicher 108, 112
Datenübernahme 183
Datenübernahmekonzept 183
Datenverarbeitungskonzept 142
Datenwerte 107
Delphi-Methode 72
Design-Fehler 178
DIN 55 350 145
DIN 62198 13, 15
DIN ISO 8402 145
DIN ISO/IEC 2383-1 107
Dokumentation 174, 184
Dokumentationsplan 130
Dokumentenprüfung 168
DriveSPI 45
Droege & Comp. 55
DV-Konzept 162
Dynamik des Marktumfeldes 76
Entität 109
Entity Relationship-Diagramme 120
Entscheidungstabellen 120
Entwicklungsmethode 60
Entwicklungsprozess 196
Entwicklungsumgebung 42, 161
Erfahrung und Sachkenntnis 83, 90
Erfolgsfaktoren 41, 51, 62
Ergebnisverantwortung 62
EUREKA 45
Externe 44, 87, 92, 93, 195
Fachkonzept 120, 125
Fehlbesetzungen 54
Fehler 171, 178
Fehlerursachen 120
Feinkonzept 142
Flexibilität 108
forsa-Institut 54
Fragebogen 71, 114
Fraunhofer-Institut 55
Frühwarnindikatoren 16, 79
Frühwarnsystem 15
Function Point 106, 128
Funktionalität 162
Funktionstest 168
Funktionstrennung 176

Gantt-Diagramme 131
Gartner Group 106
Gefährdungsindikator 31
Geschäftliche Ausrichtung 74, 116
Geschäftliche Unterstützung 74
Geschäftsbereiche 26, 74, 80, 97, 116, 135
Geschäftsprozesse 44, 94, 96, 151, 154
Geschäftsstrategie 75, 116
Geschäftsziele 10, 40, 116
GfK Marktforschung 54
Großprojekte 59
Grundprinzipien der Softwareentwicklung 62
Handlungsalternativen 198
Hardware 105, 163
Inbetriebnahme 175
Information 107
Information Systems Audit and Control Association 39
Informationsarchitektur 108
Informations-Kunden 180, 185
Infosys 58
Innovationsgrad 44
Inspektion 164
Integrationsplan 62
Integrationstest 168
Internes Kontrollsystem 15
Interviews 71, 114
ISO 12207 34
ISO 9001 34, 141
ISO/IEC TR 15504 34
Ist-Prozesse 151, 155
IT-Governance 21
IT-Strategie 75
Kennzahlen 79
Klarheit 121, 162
Kommunikation 42, 50, 53, 59
Kommunikationsaufwand 133
Kommunikationsmanagement 139
Kommunikationspfade 133
Kommunikationsplan 130
Kommunikationsverbindungen 106
Komplexität 102
Komponenten 106
Konfigurationsmanagement 61, 172, 196
Konfigurationsmanagementplan 130
Konfigurationstest 168
KonTraG 25
Kontrollen 153, 183
Ausgabe- 153
Dateneingabe- 153
nachgelagerte 181
Verarbeitungs- 153
vorbeugende 181
Kontrollziele 40
Korrektheit 121, 162
Kosten-/Nutzen-Betrachtung 123, 193
Kostenplanung 50, 130
Kostenziele 195
KPMG 49, 52, 56
Kreditwesengesetz 27

Kritikalität des IT-Systems 77
Kritische Erfolgsfaktoren 41
kritischer Pfad 50
Kundenzufriedenheit 45
Lasttest 168
Leistungsindikatoren 41
Lenkungsausschuss 134
Lieferanten 50, 57, 87, 141, 195
Lieferantenstruktur 44
Machbarkeitsstudie 119
magisches Dreieck 14, 53
Management 50, 51
Massentest 168
McKinsey Global Institute 58
Meilensteine 52, 130, 149
Migration 179
Mindestanforderungen an das Betreiben von Handelsgeschäften 26
Missbrauch 81
Mitarbeiter 44, 50, 52, 57, 60, 62, 96, 104, 138, 140, 195, 196
Modulgröße 178
Modultest 167
Monte-Carlo-Simulation 72
Motivationsmangel 60
Nachvollziehbarkeit 121
Netzplantechnik 131
Notfallvorsorge 176
Nutzen 80
Nutzervertreter 134
Objekte 106
Office of Government Commerce 43
Office of the Comptroller of the Currency 27
Ordnungsmäßigkeit der Prozesse 152
Organisationskultur 98
Organisationsstruktur 44
organisatorische Veränderungen 156
Paralleltest 169
Parkinson'sche Gesetz 129
Passivsumme 191, 194
Performance 58, 62, 163, 168, 176
Personalaufstockung 61
Personalplan 130
Pflichtenheft 120
Phasenplan 130
Planung der Datenbereitstellung 181
Priorität 53, 61
Probabilistic-Event-Analyse 72
Problem Management 144
Probleme 150
Produktentwicklung 42
Produktivität 133, 195
Produktspezifikation 61
Programmidentität 173
Programmierfehler 178
Programmiermethoden 62
Programmiersprachen 105
Programmtest 142
Programmzeilen 105, 178
Project Governance 25
Project Profile Model 44

Projekt 10
Projektaufgaben 127, 149
Projektauftrag 53
Projektbudget 123
Projektbüro 134
Projektcontrolling 18, 56
Projektdefinition 40, 82
Projektfehlläufer 50, 51, 62
Projektfreigabe 40
Projekthistorie 86
Projektinitialisierung 61
Projektkontrollen 64, 82, 113
Projektkontrollindikatoren 124, 148, 155, 159, 178, 185
Projektkosten 44, 80, 149
Projektlaufzeit 91
Projektleitfaden 37, 126
Projektmanagement 82, 125
Projektmanagementmethoden 50, 126, 127
Projektmanagementrisiko 14
Projektmanagement-Tools 131
Projektmanager 48, 50, 53, 57, 90, 134
Projektmasterplan 40
Projektmitarbeiter 92, 149
Projektorganisation 82, 126, 132, 149, 196
Projektplanung 50, 51, 53, 58, 60, 82, 129, 131, 149, 195
Projektportfolio 117
Projektrestriktionen 42
Projektrisiken 43, 54, 63
Projektrisiko 13
Projektrisikoindikatoren 79
Projektrisikomanagement 36, 40, 61, 122
Projektrisikomanager 200
Projektrisiko-Matrix 189
Projektspezifikation 119
Projektsponsor 134
Projektstandorte 92
Projektsteuerung 82, 136
Projektteam 40, 47, 50, 53, 83, 133, 197
verteiltes 140
Projektterminplanung 131
Projektüberwachung 82, 136
Projektumfang 58, 84, 91
Projektvereinbarung 127
Projektziele 14, 50, 53, 82, 118, 195
Prototyping 61, 121, 131, 160, 196
Prozessmodell 34, 42
Prozessverbesserung 62
Pseudocode 120
Qualität 107, 145, 163
Qualitätsmanagement 145
Qualitätsmerkmale 171
Qualitätssicherung 55, 60, 126, 145
Qualitätssicherungsmaßnahmen 145, 150, 196
Qualitätssicherungsplan 40, 61, 130
Quality Gate 142
Realisierung 163
Redundanzen 198
Regelkreislauf 16
Reifegrad 32, 41

Ressourcen 51, 84, 195
Ressourcenplanung 54, 130
Review 50, 121, 127, 130, 142, 160, 164
Revision 15, 153, 155
Risiko 12
Außergewöhnliches 78
Betriebs- 45
Compliance- 28
Definitions- 45
externes 14, 45
finanzielles 45, 78
inhärentes 64
Marketing- 45, 78
operationelles 30
operatives 43, 78
Organisations- 45
Organisatorisches 14
Planungs- 45
Produkt- 45
Programme 43
Projekt- 14
Prozess- 45
Reputations- 28
strategisches 28, 43, 45
Transaktions- 27
vertragliches 45
Wartungs- 45
Risikoakzeptanz 192, 199
Risikoanalyse 16, 36, 50, 187
Risikoaufschlag 198
Risikobegrenzung 192, 197
Risikobehandlungsmaßnahmen 192
Risikobericht 201
Risikobeurteilung 16, 43, 72
Risiko-Checkliste 201
Risikoeigentümer 201
Risikoerkennung 71
Risiko-Handbuch 43
Risikoidentifikation 16, 43
Risikokatalog 58, 71
Risikokategorien 32
Risikoklassen 45
Risikokommunikation 16
Risiko-Kontroll-Matrix 187
Risikomanagement 15
Risikomanagement bei IT-Projekten 17, 20
Risikomanagement-Kreislauf 63
Risikomanagementprozess 37
Risikomanagementsystem 15
Risikomaßnahmen 43
Risikometriken 201
Risikoreduktionstreppe 192
Risikoskalierung 80
Risikotoleranz 43
Risikotypen 31, 57
Risikoüberwachung 17, 36, 43, 187
Risikoursachen 57
Risikoverlagerung 192, 198
Risikovermeidung 192, 194
Risikoverminderung 192, 195

Risiko-Workshops 71
RISKMAN 45
Sachziele 195
Schlüsselpersonen 86
Schnittstellen 102, 103, 163, 168
Schulungen 100, 159
Schulungsdurchführung 158
Schulungsplanung 130, 157
scope creep 143
Servicezeiten 176
Sicherheitsmaßnahmen 153
Sicherheitstest 168
Simulation 121, 160, 196
Software Engineering Institute 32, 42
Softwarearchitektur 62
Softwareentwicklungsmethoden 50
Soll-Prozesse 152, 155
Source Code 164
SPICE 35, 45
Spiralmodell 160
Stabilität 108, 120, 162
Stabilität der Organisation 75
Stakeholder 74
Standardsoftware 20, 93, 101, 102, 173
Standish Group 47, 51
Statusberichtsplan 130
Störungsmanagement 176
Stresstest 168
Systemdokumentation 174
Systemimplementation 103
Systeminstallation 142
Systemintegration 57, 58
Systemsicherheit 176
Systemtest 142, 168
Taxonomie 42, 67
Teamgröße 133
Teammanagement 138
Technologie 50, 58, 101, 160
TechRepublic 48
Teilprojekte 85, 196
Test 179, 186
Test der Datenübernahme 182
Test der Prozesse 154
Testbarkeit 121, 163
Testdaten 166
Testdokumentation 170
Testdurchführung 167
Testendekriterien 165
Testfälle 166
Testfreigabekriterien 170
Testkonzept 165
Testmanagement 170
Testobjekte 165
Testplanung 40, 130, 165
Teststrategie 164, 170
Testszenario 166
Testumfang 166
Testziele 165
Transaktionen 96
Transaktionssumme 81

Überstunden 150
Überwachungssystem 15, 25
Umsetzbarkeit 121, 162
Unternehmenspolitik 53
Usability Test 168
Validierung 62, 161
Verfahrensdokumentation 153, 175
Verfügbarkeit 77, 82, 176
Vertrag 58, 87, 141
Vertraulichkeit 81
V-Modell 130
Vollständigkeit 120, 162
Vorgehensmodell 82, 160
Vorstudie 119
Wahrscheinlichkeitsberechnung 12
Walk-through 164
Wartung 176
Wasserfallmodell 130, 160
Wertschöpfung 59
Wettbewerbsfähigkeit 45
Wiederverwendbarkeit 108, 163
Wirkungsmatrix 191, 193
Wirkungsnetz 190
Wissensträger 86
XP 131, 160
Zeitplan 130
Zeitplanung 61
Zeitziele 195
Zieldefinition 54
Zielerreichungsindikatoren 41
Zielübereinstimmung 98