15 Risikomanagement

Risikomanagement beinhaltet die Auseinandersetzung mit Risiken. Eine der ersten Fragen, die sich hier aufdrängt, ist, warum Risiken eigentlich „gemanagt“ werden müssen und nicht einfach vermieden werden können. Kurz gesagt: Risiken und Gewinn gehen immer Hand in Hand. Wenn es in einem Projekt (fast) kein Risiko gibt, dann ist der Gewinn (Nutzen), den dieses Projekt bringt, auch sehr gering.

In einer typischen Unternehmenskultur ist Risikomanagement ein schwieriges Unterfangen, weil es zu einem offenen Umgang mit Unsicherheit ermuntert. Der Kunde eines Unternehmens zum Beispiel wäre sicher nicht erfreut, wenn ihm der Projektleiter, der die Risiken analysiert hat, mitgeteilte, dass aufgrund einiger identifizierter Risiken der beschlossene Liefertermin bei weitem nicht eingehalten werden könne. Natürlich besteht dann die Gefahr, dass der Kunde sich einen anderen Hersteller sucht, der ihm das Ausmaß der Unsicherheit nicht so direkt offenbart.

Warum dann also Risikomanagement, wenn sich Kunden dadurch abschrecken lassen?

Als Antwort auf diese Frage ein Zitat:

> *Das Maß der Unsicherheit einzugrenzen, mag manche erschrecken – es ist in der Tat nicht einfach zu akzeptieren, wie wenig Sicherheit es gibt! Unsicherheit nicht einzugrenzen, konfrontiert uns mit einem schlimmeren Übel : grenzenloser Unsicherheit. Grenzenlose Unsicherheit lässt Menschen entweder risikofeindlich oder tollkühn werden. Beide Eigenschaften können sich verheerend auswirken. [DeMarco et al, 1998]*

Im nächsten Abschnitt wird der Begriff Risiko definiert und es werden Gründe angegführt, warum Risikomanagement im Projektumfeld von Bedeutung ist. Anschließend werden die wichtigsten Aktivitäten des Risikomanagements beschrieben. Dann wird ein konkreter Ansatz, die RiskIt-Methode, detaillierter beschrieben.

15.1 Der Begriff „Risiko“

Risiko ist definiert als der – mit einer bestimmten Wahrscheinlichkeit auftretende – Verlust. Dieser Verlust kann finanziell, personell, zeitlich etc. sein. Die folgende Grafik veranschaulicht die wesentlichen Attribute eines Risikos: Wahrscheinlichkeit und Verlust(-größe). Wichtig ist dabei, dass der Verlust nur in Abhängigkeit von den definierten Zielen geschätzt werden kann. Diese Ziele wiederum werden von den verschiedenen Interessensgruppen (so genannte *Stakeholder*) in einem Projekt definiert.

Daraus ergibt sich, dass sich die Risiken während eines Projektes ändern können, wenn sich die Stakeholder (und damit vielleicht auch die Ziele) ändern.

Das wesentliche bei der Definition von Risiko ist also der Zusammenhang mit den angestrebten Zielen.

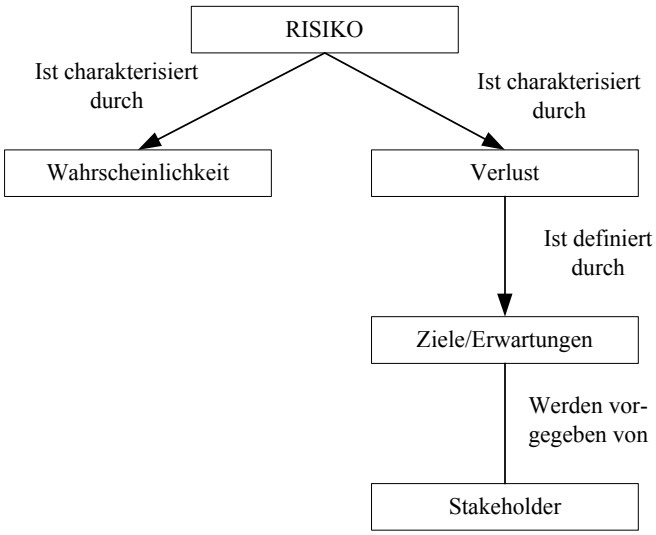

Abbildung 15.1: Definition von Risiko nach Kontio [Kontio, 2000]

Um ein Softwareprojekt erfolgreich zu beenden, ist es notwendig, Maßnahmen zu ergreifen, um potentielle Risiken nicht zu einer echten Gefahr für den Projekterfolg werden zu lassen. Diese Maßnahmen kann man zusammenfassend als Risikomanagement bezeichnen. Dies wird durch folgendes Zitat untermauert:

„ If you don’t actively attack the risks, they will actively attack you“ [Gilb, 1988]

Kritiker behaupten, dass gutes Projektmanagement schon Risikomanagement beinhaltet. Folgende Tabelle zeigt jedoch die wesentlichen Unterschiede zwischen Projektmanagement und Risikomanagement auf [Westfall].

Projektmanagement	**Risikomanagement**
Zielt auf allgemeine Risiken ab	Zielt auf die für das jeweilige Projekt speziellen Risiken ab
Überblick über den Projektverlauf	Blick auf: Spezielle Risiken
Es wird geplant, was passieren soll	Es wird analysiert was passieren kann und es werden Methoden zur Schadensminimierung gesucht
Es wird für den Projekterfolg geplant	Es wird geplant, um potentielle Verluste zu verhindern

Tabelle 15.1: Projektmanagement versus Risikomanagement

15.2 Gründe für aktives Risikomanagement

Boehm [Boehm, 1989] definiert 4 Hauptgründe für das Verwenden von Risikomanagement in einem Softwarprojekt:

- Um den finanziellen und zeitlichen Rahmen eines Projekts nicht zu überschreiten und um „*fehlergespickte*“ Software zu verhindern.
- Um „*rework*“ zu verhindern, welches üblicherweise 40-50% der Totalkosten eines Softwareprojekts ausmacht.
- Um die Suche nach Risiken in Bereichen, wo es keine relevanten Risiken gibt, zu verhindern (mit „relevant“ sind Risiken gemeint, die die in einem Projekt definierten Ziele bedrohen).
- Um eine Win-Win-Situation zu schaffen, in der der Kunde genau die Software bekommt, die er braucht und der Verkäufer genau den Gewinn macht, den er erwartet.

Risikomanagement findet nicht nur während eines Projektes statt, sondern auch vorher und nachher. So können zum Beispiel vor Projektstart Überlegungen zum Projekt gemacht werden und erste Problembereiche definiert werden usw.

Nach dem Projekt erfolgt dann die Evaluierung, bei der festgestellt wird, welche Risiken wann das Projekt bedroht haben und wie sie ausgeschaltet worden sind. Die aus der Evaluierung gewonnenen Ergebnisse können dann in spätere Projekte einfließen, um deren Ablauf zu verbessern.

15.3 Aktivitäten im Risikomanagement

Nach [DeMarco et al, 1998] setzt sich Risikomanagement im Allgemeinen aus 5 Hauptaktivitäten zusammen:

- *Risikoidentifikation*: Dieser Schritt enthält das Brainstorming über Risiken.
- Im Rahmen der *Risikobewertung* erfolgt die Quantifizierung jedes Risikos nach Eintrittswahrscheinlichkeit und Schadenshöhe.
- *Eventualfallplanung*: Hier wird beschrieben was unternommen wird, falls ein Schadensfall tatsächlich eintritt.
- *Risikoverminderung*: In diesem Schritt werden Maßnahmen erarbeitet, die vor dem Risikoeintritt erfolgen müssen, um die geplanten Maßnahmen zur Risikobewältigung im Schadensfall möglich und effektiv zu gestalten.
- *Fortlaufende Beobachtung der Eintrittsindikatoren*: Verfolgen der gemanagten Risiken und beobachten, ob ein Risiko zu einem Problem wird (ob es sich materialisiert).

Während die Risikoidentifikation eine übergreifende Aktivität darstellt, werden alle anderen Aktivitäten für jedes Risiko einzeln durchgeführt.

15.4 Das RiskIt Modell

Ein Ansatz, in dem diese 5 Aktivitäten besonders deutlich werden, ist der RiskIt-Prozeß. Die RiskIt-Methode von Jyrki Kontio [Kontio, 2000] stellt eine effektive Möglichkeit dar, Risikomanagement im Rahmen eines SE-Projektes zu betreiben, bei der die Sichten aller Interessensgruppen (Stakeholder) in einem Projekt berücksichtigt werden. Sie besteht aus 7 Schritten, die nacheinander abgearbeitet werden können, und ermöglicht somit die Identifikation, die Analyse und die Kontrolle von Risiken. Abbildung 15.2 stellt die Abfolge der einzelnen Schritte dar.

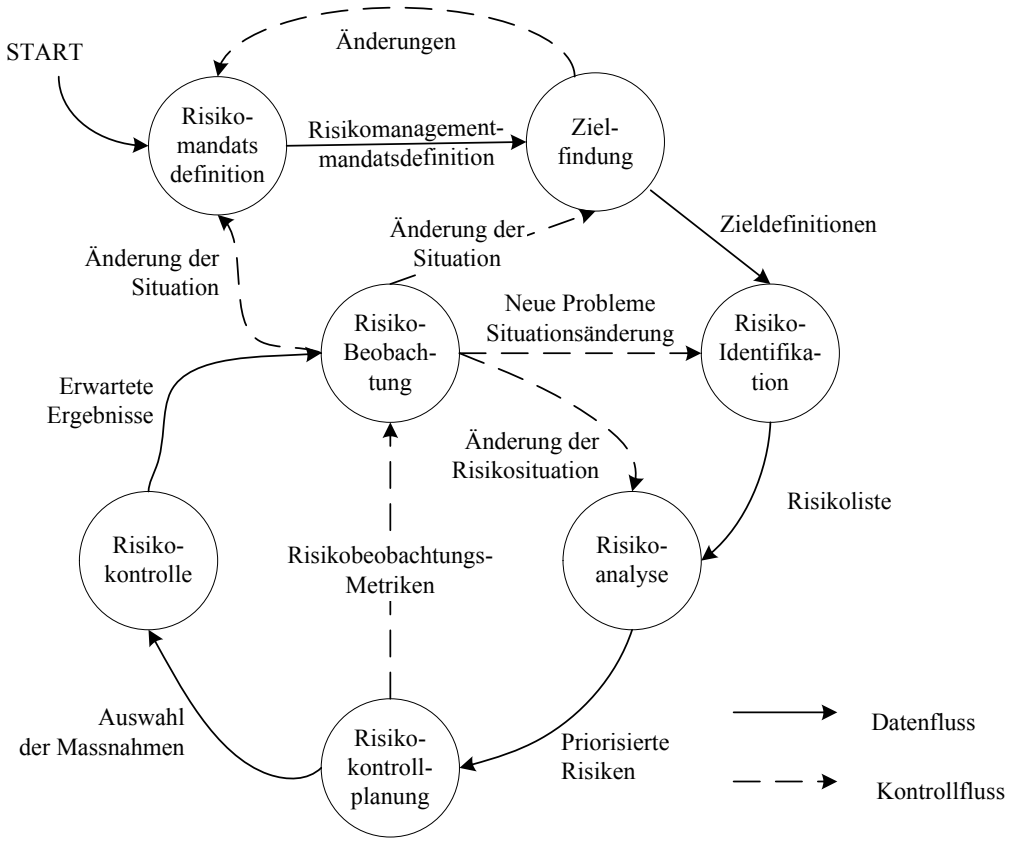

Abbildung 15.2: Überblick über den RiskIt Prozess nach Kontio [Kontio, 2000]

15.4.1 Risikomandatsdefinition

Die Risikomandatsdefinition ist der grundlegende Schritt beim Risikomanagement, bei dem festgelegt wird, ob und in welchem Ausmaß Risikomanagement (RM) innerhalb eines Projekts betrieben werden soll. Um solch ein „Mandat“ aufstellen zu können, sind Informationen über das

Projektbudget sowie über die zu Verfügung stehenden Ressourcen notwendig. Das Ergebnis ist ein Dokument, in dem u.a. festgeschrieben steht, wer die Stakeholder sind, welche Risikobereiche akzeptiert werden und in welchem Ausmaß (z.B. Personenwochen) RM-Aktivitäten vollzogen werden sollen.

15.4.2 Zielfindung

Risiken für ein Projekt lassen sich nur dann zufriedenstellend feststellen, wenn die Ziele (Goals), die im Projekt erreicht werden sollen, bekannt sind. Die Definition der Ziele der einzelnen Stakeholder ist der Inhalt der Zielfindung.

Da für mehrere Stakeholder die unterschiedlichen Ziele verschieden wichtig sind, wird bei der Zielfindung eine stakeholder-goal-priority-Tabelle angelegt, die die Wichtigkeit der Ziele für die einzelnen Stakeholder festhält. Die folgende beispielhafte Tabelle stellt eine stakeholder-goal-priority-Tabelle dar.

	Kunde (Priorität 1)	**Projektmanager (Priorität 1)**	**...**	**Entwickler (Priorität 2)**
Einhaltung des Liefertermins	1	1	…	4
Kosten niedrig halten	1	4		k.A.
Gewinn maximieren	3	1		2
…	…	…	…	…
Erweiterung der Kenntnisse in der verwendeten Programmier-sprache	k.A.	3	…	1

Tabelle 15.2: Stakeholder/Goal-priority-Tabelle [Kontio, 2000]

Das obige Beispiel zeigt: Das Ziel „Einhaltung des Liefertermins“ ist sowohl für den Kunden, als auch für den Projektmanager von besonderer Bedeutung, für den Entwickler hingegen kaum (nur Priorität 4 bei Entwickler).

Aus der Tabelle lassen sich auch schon erste Konflikte identifizieren: so ist ein Hauptziel des Kunden, die Kosten niedrig zu halten, und ein Ziel des Projektmanagers, den Gewinn zu maximieren.

15.4.3 Risikoidentifikation

Nachdem die Ziele definiert worden sind, werden in diesem Schritt die Risiken, die das Projekt gefährden, identifiziert und in einer Liste zusammengefasst. Diese Liste sagt noch nichts über die Priorität der einzelnen Risken aus.

Einige Methoden der Risikoidentifikation seien hier der Vollständigkeit halber erwähnt: Interviewing, Brainstorming, Voluntary Reporting, Decomposition, Assumption Analysis, Critical Path Analysis, Risikotaxonomien, Checklisten. Der „Output" der Risikoidentifikation ist also eine ungeordnete Liste aller für das Projekt relevanten Risiken.

15.4.4 Risikoanalyse

Die ungeordnete Liste der Risiken, die in der Risikoidentifikation gefunden wurden, wird nun genauer untersucht, damit eine Reihung dieser Risiken nach Wichtigkeit erfolgen kann. Da für das Risikomanagement üblicherweise nur begrenzt Zeit und Ressourcen zu Verfügung stehen, werden im weiteren Ablauf nur die wichtigsten Risiken berücksichtigt. Das Werkzeug, das zur Analyse verwendet wird, ist der RiskIt Analysis Graph, dessen Verständnis für die Risikoanalyse wesentlich ist.

Der RiskIt Analysis Graph ist eine Möglichkeit, alle risikobezogenen Informationen auf eine strukturierte Art und Weise darzustellen. Der Graph besteht aus verschiedenen *risk elements*: *risk factors*, *risk events*, *risk outcome*, *risk reaction* und *effects*. Der Zusammenhang dieser Elemente wird in der folgenden Abbildung dargestellt.

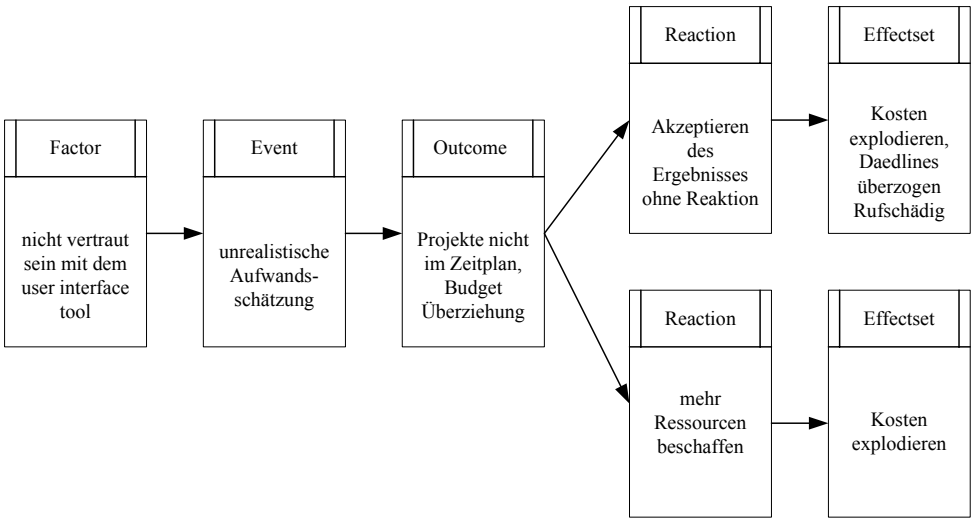

Abbildung 15.3: Beispiel für einen RiskIt Analysis Graph

Risk factors sind bekannte Tatsachen über eine Situation, *risk events* sind Ereignisse, die negative Folgen für das Projekt haben, *risk outcome* ist die Situation, die durch das Auftreten eines *risk*

events entsteht, *risk reactions* sind Tätigkeiten, die durchgeführt werden, um dem aufgetretenen Risiko entgegenzuwirken und *risk effect* ist die Auswirkung des risk events, inklusive darauffolgende Reaktionen, auf die Projektziele.

Die Risikoanalyse selbst läuft in drei Schritten ab: *Risikoclustering*, *Entwicklung von Risikoszenarien* und *Risikopriorisierung*. Risikoclustering ist vor allem dann von Bedeutung, wenn die Menge der gefundenen Risiken besonders groß ist. Die einzelnen Risiken werden in Gruppen (Cluster) mit ähnlichen Eigenschaften zusammengefasst. Risiken können zum Beispiel nach Typ oder nach Stakeholdern zusammengefasst werden. Im ersten Fall bilden technische Risiken einen Cluster, personelle Risiken einen anderen Cluster usw.

Da für die Risikoanalyse für gewöhnlich nur begrenzt Zeit zur Verfügung steht, können nicht alle in der Risikoidentifikation gefundenen Risiken zur Analyse herangezogen werden. Es muss also schon vor der eigentlichen Analyse eine Auswahl getroffen werden, welche Risiken zur Erstellung von Risikoszenarien verwendet werden. Die Entwicklung von Risikoszenarien kann beendet werden, wenn die Entwicklung neuer Szenarien nicht mehr zu neuen Kontrollaktionen führt, d.h. alle notwendigen Kontrollaktionen sind bereits definiert. Mittels des RiskIt Analysis Graphen werden Risikoszenarien definiert. Dabei werden die zur Verfügung stehenden Risiken einzelnen Risikoelementen (Risk factors,...) zugeordnet. Die daraus entstandenen Risiko Elemente werden dann zu Risikoszenarien „vernetzt“. Der resultierende RiskIt Analysis Graph beinhaltet dann alle definierten Risikoszenarien.

Wegen der bereits erwähnten zeitlichen Begrenzung für die Risikoanalyse ist es sinnvoll, nicht alle definierten Risikoszenarien zu managen, sondern nur die wichtigsten. Dazu muss eine Reihung der in der Risikoszenarienentwicklung erstellten Risikoszenarien vorgenommen werden. Diese Reihung erfolgt aufgrund von Schätzungen der Wahrscheinlichkeit, mit der das Szenario eintritt, und aufgrund von Schätzungen des Verlusts, den ein Szenario anrichten kann. So haben Risikoszenarien, die sehr wahrscheinlich eintreten werden, und die einen sehr großen Verlust anrichten, eine höhere Priorität als Szenarien, die wahrscheinlich nicht eintreten werden und auch nur einen geringen Verlust anrichten würden.

Das Endergebnis ist eine Liste, in der die vorhandenen Risikoszenarien nach Priorität geordnet sind.

15.4.5 Risikokontrollplanung

Das Ziel der Risikokontrollplanung ist herauszufinden, welche Maßnahmen getroffen werden müssen, um den in der Risikoanalyse als am gefährlichsten identifizierten Risken entgegenzuwirken.

Dieser Schritt besteht aus 2 Teilen, die parallel ablaufen können:

- *Definition von Maßnahmen*: Nach der Bestimmung der wichtigsten Risikoszenarien, kann dieser Schritt – die Definition von entgegenwirkenden Maßnahmen – als kreativer Prozess ohne starren Rahmen durchgeführt werden.
- *Auswahl der kosteneffektivsten Maßnahmen zur Umsetzung*: Nach der Definition der Risikokontrollmaßnahmen, geht es nun darum, die effektivsten Maßnahmen auszuwählen und

umzusetzen. Optimalerweise werden mehr Maßnahmen definiert als letztendlich ausgewählt werden. Das garantiert, dass alle Risikobereiche genügend berücksichtigt wurden.

Für die Auswahl der Risikokontrollmaßnahmen können u.a. folgende Kriterien herangezogen werden: Ranking der Risikoszenarien, Verfügbarkeit der notwendigen Ressourcen, usw.

Zusammenfassend sei gesagt, dass dies keine objektiven Kriterien sind, sondern dass die subjektive Einschätzung und Erfahrung der Verantwortlichen ein wesentlicher Einflussfaktor ist.

15.4.6 Risikokontrolle

Sobald die Risikokontrollmaßnahmen ausgewählt wurden, sind sie Bestandteil des Projektmanagements, das sich mit der Durchführung und Kontrolle dieser Maßnahmen beschäftigt.

Beispiel: Einer der Hauptrisikofaktoren bei IT-Projekten ist ein Personalwechsel. Eine Risikokontrollmaßnahme, um dieses Risiko zu managen, wäre, von Anfang an mit einer leichten personellen Überkapazität zu arbeiten, wobei die voll qualifizierten Zusatzleute vorübergehend die Rollen von Hilfskräften und Praktikanten einnehmen. Scheidet ein Mitarbeiter aus, braucht das Management keine neuen Leute einzustellen. Einer der Ersatzleute kann aufsteigen und die Aufgaben des ausgeschiedenen Mitarbeiters übernehmen. Der Zeitaufwand für den Wechsel ist dadurch minimal, da der „neue“ Mitarbeiter sich nicht mehr einarbeiten muß.

15.4.7 Risikobeobachtung

Die Risikobeobachtung (*risk monitoring*, *risk tracking*) ist ein kontinuierlicher Prozess, der den Status des Projekts überwacht. In regelmäßigen Zyklen (wöchentlich, zweiwöchentlich) beraten die Projektmitglieder, ob korrigierende Maßnahmen gesetzt werden müssen oder ob das Projekt reibungslos abläuft. Sobald der Eintritt eines Risikos registriert wird, werden die entsprechenden Kontrollmaßnahmen gesetzt.

Beispiel: Dem Beispiel von oben folgend würde durch die Risikobeobachtung mitten im Projekt festgestellt werden, dass ein besonders wichtiger Mitarbeiter wegen eines verlockenden Jobangebotes die Firma verlässt. Dadurch, dass sich dieses Risiko nun materialisiert, wird der Einsatz von Kontrollmaßnahmen notwendig und einer der Zusatzleute rückt an die freigewordene Stelle nach.

15.5 Zusammenfassung

Risiko ist definiert als der mit einer bestimmten Wahrscheinlichkeit auftretende (finanzielle, personelle, zeitliche) Verlust. Wesentlich bei der Definition von Risiko ist der *Zusammenhang mit den angestrebten Zielen*.

Nach De Marco setzt sich Risikomanagement im Allgemeinen aus 5 Hauptaktivitäten zusammen: *Risikoidentifikation* , *Risikobewertung*, *Eventualfallplanung*, *Risikoverminderung* und *fortlaufende Beobachtung der Eintrittsindikatoren.*

Der größte Vorzug des Risikomanagements besteht darin, dass die in einem Projekt bestehende Unsicherheit eingegrenzt wird, was für einen erfolgreichen Projektabschluss Vorraussetzung ist. Die Kernaktivitäten des Risikomanagements sind Risikoidentifikation, Risikobewertung, Eventualfallplanung, Risikoverminderung und die fortlaufende Beobachtung der Eintrittsindikatoren.

Eine effektive Möglichkeit, Risikomanagement im Rahmen eines SE-Projektes zu betreiben, stellt die *aus 7 Schritten (Risikomandatsdefinition, Zielfindung, Risikoidentifikation, Risikoanalyse, Risikokontrollplanung, Risikokontrolle, Risikobeobachtung)* bestehende *RiskIt-Methode* von Kontio dar, bei der die Sichten aller Interessensgruppen (Stakeholder) in einem Projekt berücksichtigt werden (siehe [Kontio, 2000]).

15.6 Literaturreferenzen

[Boehm, 1989] Böhm, Barry W: Software Risk Management, IEEE Computer Society Press, 1989.

[Carr et al, 1993] Carr, M.; Kondra S.; Monarch, I.; Ulrich, F.; Walker, C.: Taxonomy-Based Risk Identification, Tech. Rep. CMU/SEI-93-TR-006, Software Engineering Institute, 1993.

[Charette, 2000] Charette, Robert N.: The New Risk Management, Cutter Consortium Executive Report, Business IT Strategies Advisory Service, Vol. 3, No. 9 (2000).

[Charette, 1989] Charette, Robert N.: Software Engineering Risk Analysis and Management, New York: McGraw-Hill, 1989.

[DeMarco et al, 2003] DeMarco, Tom; Lister, Timothy: Bärentango. Mit Risikomanagement Projekte zum Erfolg führen; Hanser Fachbuch; 2003-11-25.

[Fairley, 1994] Fairley, R.: Risk Management for Software Projects, IEEE Software, Vol. 11, No. 3 (May 1994), pp. 57-67.

[Grey, 1995] Grey, Stephen: Practical Risk Assessment for Project Management, Wiley Series in Software Engineering Practice, John Wiley & Sons Ltd., 1995.

[Hall, 1998] Hall, E.: Managing Risk: Methods for Software Systems Development, Reading, Mass.: Addison-Wesley, 1998.

[IEEE Computer Society, 1997] IEEE Computer Society, Managing Risk, IEEE Software, Vol. 14, No.3 (May/June 1997).

[Jones, 1994] Jones, Capers: Assessment and Control of Software Risks (Yourdon Press Computing), Prentice Hall PTR, 1st edition (February 1994).

[Karolak, 2002] Karolak, Dale Walter: Software Engineering Risk Management, ISBN: 0-8186-7194-7.

[Kontio, 2000] Kontio, J.: The Riskit Method for Software Risk Management, Version 1.00, CS-TR-3782, 1997. Computer Science Technical Reports. University of Maryland. College Park, MD. http://www.soberit.hut.fi/~jkontio/riskittr.pdf

[Kontio et al, 1998] Kontio, J.; Getto, G.; Landes, D.: Experiences in improving risk management processes using the concepts of the Riskit method. Proceedings of the Proceedings of the Sixth International Symposium on the Foundations of Software Engineering (FSE-6), 1998.

[Rosenthal et al, 1991] Rosenthal, Robert; Rosnow, Ralph L.: Essentials of Behavioral Research: Methods and Data Analysis, McGraw-Hill Humanities/Social Sciences/Languages; 2nd edition (January 1, 1991), ISBN: 0070539294.

15.7 Übungen und Fragen

1. Was ist Risiko? Welche Hauptgründe gibt es Risiken im Projektumfeld zu analysieren?
2. Nenne drei Beispiele, die die Ziele von verschiedenen Stakeholdern einen zu erwartenden Verlust definieren können.
3. Wie spielen Projekt- und Risikomanagement zusammen? Welche Stakeholder sind auf welcher Ebene beteiligt?
4. Nenne die relevanten Aktivitäten im Risikomanagement. Nenne ein Beipiel für ein konkretes Prozessmodell.
5. Was versteht man unter Risikomandatdefinition?
6. Nenne die drei Hauptschritte im Analyseteil von Kontios Riskit-Prozess.
7. Warum ist Risikobeobachtung notwendig? Nenne ein konkretes Beispiel.