

Spotlight

Risikomanagement in der Praxis



Eine themenspezifische Zusammenstellung der besten, auf projektmagazin.de erschienenen Artikel, Methoden und Tipps.

www.projektmagazin.de

Mehlbeerenstr. 4, 82024 Taufkirchen

Tel: +49 89 2420798-0

Fax: +49 89 2420798-8

Risikomanagement in der Praxis

Risikoidentifikation, Risikoanalyse, Risikomatrix – im aktuellen E-Book erhalten Sie das methodische Handwerkszeug für erfolgreiches Risikomanagement. Sie erfahren, wie Sie in der Praxis mit Risiken umgehen können und worauf Sie dabei achten sollten. Mit speziellen Anwendungsbeispielen zeigen wir Ihnen die Bandbreite des Risikomanagements in Projekten auf.

Inhalt

Methoden für den Umgang mit Risiken

1. Risikomanagementverfahren Seite 3
2. Risikoidentifikation Seite 16
3. Risikoanalyse Seite 24
4. Risikomatrix Seite 34
5. Risikokatalog Seite 41

Anwendungsbeispiele für Risikomanagement

6. Fehler vermeiden statt aufwendig beseitigen
Mit FMEA auf der sicheren Seite – ein Praxisbeispiel..... Seite 49
7. Herausforderung und Verantwortung für jeden einzelnen
Informationssicherheit und Projekte..... Seite 64
8. Pragmatisches Bestimmen der Kritikalität von Lieferanten und deren Bauteilen
Risikomanagement in der Supply Chain Seite 76
9. Verfahren zur Risikoanalyse am Beispiel DESERTEC
Abbildung von Risiken in Großprojekten oder was Risiken und Cocktails gemeinsam haben Seite 85
10. Wenn man vor lauter Bäumen den Wald nicht mehr sieht
Die 4 Os zur Risikoidentifikation in Großprojekten..... Seite 99

Risikomanagementverfahren



Ein Risikomanagementverfahren verbindet die einzelnen Methoden des Risikomanagements zu einem kontinuierlich ablaufenden Projektmanagementprozess. Unsicherheit ist ein Charakteristikum von Projekten. Deshalb benötigt das Management von Projekten ein integriertes Verfahren zur Überwachung und Steuerung von Chancen und Bedrohungen.

Einsatzmöglichkeiten

- Risikomanagement in Teilprojekten, Projekten, Programmen und Projektportfolios
- Für das Risikomanagementverfahren muss eine verantwortliche Person benannt werden. Im Regelfall ist dies der Projektmanager. Die Durchführung des Risikomanagementverfahrens ist Aufgabe mindestens des Projektmanagementteams, nach Möglichkeit ist das gesamte Projektteam einzubinden.
- Aufwand und Schwierigkeitsgrad des Risikomanagementverfahrens richten sich nach Umfang und Komplexität des Projekts.

Vorteile

- Umfang und Detailliertheit des Risikomanagements werden an die Anforderungen des Projekts und seines Umfelds angepasst. Dies vermeidet unnötige Aufwände und gewährleistet ausreichende Risikovorsorge.
- Die Verantwortlichkeiten für die Risikoüberwachung und –behandlung werden definiert. Dies gewährleistet klare Kommunikation und unverzügliches Handeln.
- Die Risikobelastung des Projekts wird steuerbar

- Der Einsatz eines definierten Verfahrens erlaubt eine kontinuierliche Verbesserung des Risikomanagements.
- Die Stakeholder sind sowohl über Chancen als auch Bedrohungen des Projekts informiert und können ihre Entscheidungen danach ausrichten

Grenzen, Risiken, Nachteile

- Die Wirksamkeit des Risikomanagements innerhalb eines Projekts wird begrenzt durch die Qualität des Risikomanagements in dessen Trägerorganisation.
- Aktiv betriebenes Risikomanagement kann dazu führen, dass die Risikobereitschaft von Entscheidern sinkt, da die Risikobelastung dokumentiert und für alle Stakeholder transparent wird.

Ergebnis

- Stets aktuelle Risikoliste des Projekts
- Liste der beschlossenen Risikomaßnahmen
- Klare Verantwortlichkeiten für die Behandlung von Risiken
- Stets aktuelle Darstellung der Risikobelastung des Projekts als Input für Entscheidungen des Lenkungsausschusses

Voraussetzungen

- Bereitschaft der Organisation, Risiken in einem transparenten und nach Objektivität strebenden Verfahren zu managen
- Es liegt eine klare Definition des Projektziels vor (z.B. in Form eines Business Cases)

Qualifizierung

Die erforderliche Qualifikation zur Durchführung eines Risikomanagementverfahrens ist von den Anforderungen des Projekts und seines Umfelds abhängig. In Projekten mit geringen Unsicherheiten sind keine besonderen Kenntnisse erforderlich. Bei Umfeldern mit hohen Unsicherheiten und in Trägerorganisationen mit geringer Risikobereitschaft kann eine Qualifizierung für Risikomanagement erforderlich sein.

Benötigte Informationen

- Bestehende Risikomanagementsysteme von Auftraggeber und Auftragnehmer
- Projektinformationen, z.B. Projekthandbuch, Projektauftrag, Pläne

- Informationen über Projektumfeld
- Ggf. Expertenwissen für spezifische Fragen
- Kommunikationsplan mit Stakeholderliste

Benötigte Hilfsmittel

- Risikoliste (Risikoregister, Risikoverzeichnis) des Projekts
- Projektkommunikationsmittel wie z.B. Kollaborationsportal, Verteilerlisten
- Hilfsmittel für die jeweils eingesetzten Methoden

Durchführung

- Analysieren Sie das Umfeld!
- Definieren Sie das Risikomanagementsystem für Ihr Projekt!
- Implementieren Sie das Risikomanagementverfahren in Ihrem Projekt!
- Schritt 1: Identifizieren Sie die Risiken!
- Schritt 2: Analysieren und bewerten Sie die Risiken!
- Schritt 3: Planen Sie die Risikomaßnahmen!
- Schritt 4: Benennen Sie die Risikoverantwortlichen!
- Schritt 5: Setzen Sie die Maßnahmen um oder planen Sie ihre Umsetzung!
- Kommunizieren Sie beständig Risiken und Maßnahmen an die Stakeholder!
- Ergänzende / ähnliche Methoden

Risiken sind hinsichtlich Eintrittswahrscheinlichkeit und Auswirkung bewertete, zukünftige Ereignisse, die bei ihrem Eintreten ursächlich eine Abweichung der Ist-Daten von den Plandaten bewirken. Diese Abweichungen können sowohl negative als auch positive Effekte haben. Dementsprechend werden Risiken unterschieden nach Bedrohungen und Chancen.

Im allgemeinen Sprachgebrauch werden die Begriffe "Risiko" und "Bedrohung" meist gleichgesetzt. Die Richtlinien für Risikomanagement und Projektmanagement betrachten jedoch Risiken allgemein als ungewisse, in der Zukunft liegende Ereignisse, die sich positiv wie negativ auf die Projektziele auswirken können. Die folgende Darstellung beschäftigt sich deshalb zwar hauptsächlich mit Bedrohungen, berücksichtigt aber auch so weit als möglich das Management von Chancen.

Analysieren Sie das Umfeld!

Das Projektumfeld ist die wichtigste Quelle für Unsicherheiten, da es nicht durch das Projektmanagementteam gesteuert werden kann. Liegen noch keine Umfeld- und Stakeholderanalyse vor, führen Sie diese Analysen als erstes durch.

Hierfür stehen Ihnen drei Methoden zur Verfügung: **Umfeldanalyse**, **Stakeholdermanagement** und **Lessons Learned**. Umfeldanalyse und Stakeholdermanagement weisen einige Überschneidungen auf. Sie können die beiden Methoden kombinieren oder sich auf nur eine beschränken, je nach Komplexität Ihres Projekts. Gibt es bereits eine etablierte Sammlung von Erfahrungswerten, können Sie direkt auf die dort dokumentierten Lessons Learned zugreifen, die sich auf Ihr spezifisches Projektumfeld beziehen. Ansonsten ist es empfehlenswert, mit Hilfe der Methode Lessons Learned gezielt die Erfahrungen von Beteiligten ähnlicher Projekte hinsichtlich Umfeldeinflüssen abzufragen.

Definieren Sie das Risikomanagementsystem für Ihr Projekt!

Je nachdem, ob Ihr Projekt die Steuerungssoftware für ein Passagierflugzeug oder ein innerbetriebliches Konzept für die Vereinbarkeit von Familie und Beruf entwickeln soll, brauchen Sie vollkommen unterschiedliche Ansätze für das Risikomanagement. Genauso wie für Qualität oder das Projektmanagement selbst benötigen Sie ein Managementsystem für Risiken. Dafür gibt es in der Literatur und den Richtlinien unterschiedliche Bezeichnungen: Der PMBOK® Guide (PMI) nennt es Risikomanagementplan, PRINCE2® (AXELOS) Risikomanagementstrategie bzw. Risikomanagement-Ansatz und die ICB 4.0 (IPMA) Risikomanagementstruktur.

Elemente eines Risikomanagementsystems

Ohne Anspruch auf Vollständigkeit finden Sie im Folgenden eine Auflistung von typischen Elementen eines Risikomanagementsystems, die Sie für Ihr Projekt definieren sollten.

Rollenbeschreibungen

Grundsätzlich ist der Projektmanager für das gesamte Risikomanagement im Projekt verantwortlich. Je nach Umfang und Anforderungen des Projekts ist es sinnvoll oder notwendig explizite Rollen für das Risikomanagement zu definieren und an Projektbeteiligte zu delegieren.

Definieren Sie Aufgaben, Verantwortungen und Befugnisse für die in Ihrem Projekt erforderlichen Rollen des Risikomanagements. Dies können z.B. sein:

- **Risikomanager:** Hauptverantwortlicher für das gesamte Risikomanagement des Projekts als delegierte Aufgabe des Projektmanagers
- **Risikoeigentümer:** Verantwortlicher für die Überwachung eines oder mehrerer Risiken
- **Risikobearbeiter:** Ausführender einer Risikomaßnahme nach Beauftragung durch den Risikoeigentümer.

Risikobereitschaft des Auftraggebers oder der Trägerorganisation

Zur Steuerung der Risikosituation eines Projekts ist die wichtigste Eingangsgröße die Bereitschaft des Auftraggebers bzw. der Trägerorganisation, Unsicherheiten in Kauf zu nehmen.

Die Risikobereitschaft kann dabei nicht durch eine einzige Zahl ausgedrückt werden. Zum einen verändert sich die Risikosituation während des Projektablaufs zum anderen müssen zu ihrer Beurteilung stets mehrere Szenarien betrachtet werden. Hierzu steht die Methode **Szenariotechnik** zur Verfügung.

Um die Risikobereitschaft zu beschreiben eignen sich z.B. folgende Angaben:

- Geforderte Erfolgswahrscheinlichkeit des Projekts im Projektverlauf (z.B. 50% bei Start, 90% nach der ersten Phase)
- Maximal geduldeter Schaden beim Scheitern des Projekts
- Maximal geduldetes Produkt aus Schadenshöhe und Eintrittswahrscheinlichkeit für ein einzelnes Risiko
- Maximal geduldete Summe aller Risikobewertungen

Um die Risikobereitschaft zu beschreiben, können wesentlich komplexere Größen erforderlich sein, die sich z.B. aus Simulationen ergeben, die die Abhängigkeiten zwischen den Risikoereignissen berücksichtigen.

Risikobudget

Es empfiehlt sich, bereits zu Beginn des Projekts einen Teil des Budgets ausschließlich zur Behandlung von Risiken zu definieren. Dies macht zum einen gegenüber dem Auftraggeber am deutlichsten klar, dass das Projekt Unsicherheiten aufweist. Zum anderen versetzt ein Risikobudget den Projektmanager in die Lage, bei eingetretenen Risiken handlungsfähig zu bleiben.

Risikomanagementverfahren

Herzstück des Risikomanagementsystems ist die Prozessdefinition, wie Risiken identifiziert und gesteuert werden. Definieren Sie das für Ihr Projekt angemessene Risikomanagementverfahren auf Basis der Schritte 1 bis 5 dieser Methodenbeschreibung.

Metriken

Risiken müssen mindestens nach Eintrittswahrscheinlichkeit und Auswirkung bewertet werden. Hierfür ist es sinnvoll, geeignete Skalen für die quantitative Bewertung zu definieren. Weit verbreitet sind drei- und fünfstufige Skalen, da es meist nicht möglich ist, diese Größen präzise zu ermitteln. Je nach Bedarf sind auch andere Metriken zu definieren, z.B. für die Eintrittsnähe oder die Wahrscheinlichkeit, dass es nicht erkannt wird. Weiterführende Hinweise zu den Bewertungsmetriken und ihrer Interpretation finden Sie in der Methode **Risikomatrix**.

Kategorien

Zur Unterstützung der Risikoanalyse und der Risikobehandlung kann es sinnvoll sein, Kategorien für Risiken und Maßnahmen zu definieren. Beispiele für Maßnahmenkategorien sind in "Schritt 3: Planen Sie die Risikomaßnahmen" aufgeführt.

Eskalationsmechanismen

Risiken können von allen Projektbeteiligten entdeckt werden. Damit diese Beobachtungen auch zu einer effizienten Risikobearbeitung führen, brauchen die Projektbeteiligten eine Möglichkeit, ihre Beobachtungen an jemanden weiterzugeben, der sie im Zusammenhang analysieren und beurteilen kann. Definieren Sie deshalb geeignete Kommunikationsprozesse, die gewährleisten, dass kein Bedenken unbeachtet bleibt. Das einfachste Verfahren ist das Prinzip der Offenen Punkte bei PRINCE2®, nachdem jeder Projektbeteiligte ein Anliegen an den Projektmanager melden kann.

Speziell PRINCE2®: Schwellenwerte festlegen

PRINCE2® behandelt die Risikobelastung des Projekts als Steuerungsgröße. Dementsprechend fordert es die Angabe von Schwellenwerten, deren Überschreitung eine Eskalation an den Lenkungsausschuss notwendig macht. Hierfür verwendet PRINCE2® den Begriff "Risikotoleranz".

Implementieren Sie das Risikomanagementverfahren im Projekt!

Damit das Risikomanagementverfahren seine beabsichtigte Wirkung erzielt, muss es nahtlos im Projektablauf integriert sein. Überprüfen Sie die anderen Projektmanagementprozesse hinsichtlich ihrer Relevanz für Risikoidentifikation, Risikoüberwachung und Risikovorsorge. Stellen Sie dann sicher, dass bei den entsprechenden Prozessschritten die jeweiligen Elemente des Risikomanagementverfahrens integriert sind. Besonders wichtig sind dabei die drei Aufgaben Planen, Entscheiden und Prüfen.

Planen

Bei allen Planungstätigkeiten ist die Risikoidentifikation zu integrieren. Zu jedem erstellten Plan sind mindestens zwei Fragen zu stellen:

- Unter welchen Voraussetzungen kann der Plan durchgeführt werden? (z.B. rechtzeitige Lieferung eines benötigten Produkts)
- Auf welchen Annahmen beruht der Plan? (z.B. Frostfreiheit für Außenarbeiten)

Sowohl Voraussetzungen als auch Annahmen müssen als Risiken analysiert werden: Mit welcher Wahrscheinlichkeit werden sie besser oder schlechter als prognostiziert eintreten?

Entscheiden

Jede Entscheidung birgt natürlich per se die Unsicherheit, dass die jeweils andere Option besser gewesen wäre. Weit wichtiger aber ist die Analyse, welche Unsicherheiten mit den in Frage kommenden Optionen verbunden sind. Es ist durchaus möglich, dass eine zunächst sehr attraktiv aussehende Option (Erweiterung des

Produkts um eine innovative Funktion) eine Reihe großer Bedrohungen (Fehlfunktion mit Schaden beim Benutzer) nach sich zieht, die mit einer anderen Option vermieden werden können. Umgekehrt kann eine zunächst weniger interessante Option (Produkt wie geplant auf den Markt bringen) große Chancen (Erhöhung des Marktanteils durch frühen Markteintritt) bieten

Bei Entscheidungen aller Art, insbesondere bei Änderungsanträgen, sind daher die Risiken der betrachteten Optionen zu identifizieren und zu bewerten. Beim **Änderungssteuerungsverfahren nach PRINCE2®** ist dies bereits integriert.

Die Methode **Entscheidungsrisikoanalyse** liefert speziell für Entscheidungssituationen ein Vorgehen, um die mit den bestehenden Optionen verbundenen Bedrohungen zu identifizieren und zu bearbeiten.

Prüfen

Jegliches Prüfen in Projekten bedeutet einen Vergleich zwischen Plan und Ist. Dabei festgestellte Abweichungen außerhalb der Toleranzen sind grundsätzlich eingetretene Risiken – auch dann, wenn sie in dieser Form nicht in der Risikoliste stehen. Prüfungsprotokolle sollten deshalb den jeweils zuständigen Risikoverantwortlichen (z.B. dem Eigentümer der mit dem geprüften Produkt verbundenen Risiken) gegeben werden, damit diese die entsprechenden Risiken neu bewerten bzw. die für den Risikoeintritt vorbereiteten Maßnahmen anordnen können.

Schritt 1: Identifizieren Sie Risiken!

Auch wenn das Identifizieren der Risiken als erster Schritt des Risikomanagementverfahrens dargestellt wird, muss es als kontinuierliche Aufgabe aufgefasst werden. Beim Initiieren und Planen eines Projekts ist es natürlich notwendig, die Risikoidentifikation als eigene Aufgabe durchzuführen, z.B. mit einem Workshop. Hierfür steht Ihnen die Methode **Risikoidentifikation** als Anleitung zur Verfügung. Bei Bedarf kann eine Wiederholung eines solchen Workshops sinnvoll sein, z.B. bei Phasenübergängen oder wenn sich das Projektumfeld stark ändert.

Eine Unterstützung für die kontinuierliche Risikoidentifikation bietet die Methode **Risikokatalog**.

Die Risikomanagementstrategie (s.o.) beschreibt, wie die Risikoidentifikation im Projektablauf integriert ist.

Schritt 2: Analysieren und bewerten Sie die Risiken!

Insbesondere für die Analyse von Risiken gibt es zahlreiche, z.T. branchenspezifische Methoden. Eine allgemeine Beschreibung des Vorgehens liefert Ihnen die Methode **Risikoanalyse**.

Zur detaillierten Analyse einzelner Risiken, die Sie für besonders relevant halten, stehen Ihnen das **Ishikawa-Diagramm** und die Methode **Negativer / Positiver Zweig** zur Verfügung.

Die aufwendigste Methode zur Risikoanalyse ist die **Fehlermöglichkeits- und Einflussanalyse (FMEA)**. Diese stammt aus dem Maschinenbau, kann aber auch z.B. in der Software-Entwicklung eingesetzt werden. Sie kommt immer dann zum Einsatz, wenn Produkte in Versionen und Varianten entwickelt werden und die vollständige Vermeidung von Fehlern das Ziel ist.

Die **Fehlerbaumanalyse** stellt eine weitere Alternative zur Analyse von Fehlerketten dar und kann insbesondere mit der FMEA kombiniert werden.

Das einfachste Vorgehen bei der Risikoanalyse ist es, für jedes identifizierte Risiko drei weitere Angaben zu machen:

- Risikoauswirkung: Worin besteht der Schaden bzw. der Nutzen?
- Risikoereignis: Was ist der unmittelbare Auslöser, der zur Risikoauswirkung führt?
- Risikoursache: Was ist der Grund dafür, dass das Risikoereignis eintreten kann?

Beispiel: Für das Risiko "die Open-Air-Veranstaltung fällt witterungsbedingt aus" ist die Risikoursache, dass die Veranstaltung im Freien stattfindet und damit dem Wetter ausgesetzt ist. Das Risikoereignis kann z.B. ein Sturm sein (Regen wäre ein anderes Risikoereignis, das auch anders zu bewerten ist). Die Risikoauswirkungen bei Sturm sind zum einen Schäden oder sogar Zerstörung der Aufbauten bis hin zu Verletzungen oder sogar Todesfällen bei den Teilnehmern. Bei Regen wären die Auswirkungen wesentlich weniger dramatisch.

Schritt 3: Planen Sie die Risikomaßnahmen!

Planen Sie zu jedem erkannten Risiko geeignete Maßnahmen, um es seiner Bedeutung gemäß steuern zu können. Aus der Risikoanalyse erhalten Sie mögliche Ansatzpunkte, um die Risiken zu beeinflussen, z.B. indem Sie Ursachen für Bedrohungen beseitigen.

Maßnahmenkategorien für Bedrohungen

Bei der Suche nach Maßnahmen zur Behandlung von Risiken hat es sich bewährt, sich von Kategorien anregen zu lassen. Es gibt unterschiedliche Listen solcher Maßnahmenkategorien, die zum Teil unterschiedliche Interpretationen haben. Betrachten Sie die folgenden Kategorien deshalb als Anregung, eine eigene Liste zu erstellen und seien Sie nicht überrascht, wenn Sie in PM-Richtlinien andere Kategorien und andere Interpretationen derselben Kategorie lesen.

Akzeptieren

Vor allem für Risiken mit sehr geringer Auswirkung oder extrem niedriger Wahrscheinlichkeit wäre der Aufwand für eine aktive Behandlung oft zu hoch. Das Akzeptieren einer Bedrohung bedeutet jedoch nicht, sie außer Acht zu lassen. Die Bedrohung wird selbstverständlich in der Risikoliste erfasst und einem Risikoverantwortlichen zugewiesen, da es genau wie jedes andere Risiko überwacht und ggf. neu bewertet werden muss.

Verhindern

Die erfolgreichste Maßnahme gegen eine Bedrohung ist, wenn man sie vollständig verhindern kann. Dies kann dadurch geschehen, dass ihre Ursachen vollständig beseitigt werden oder dass ein anderer Lösungsweg beschritten wird, für den die betrachtete Bedrohung irrelevant ist.

Verringern der Eintrittswahrscheinlichkeit

Wenn eine Bedrohung nicht vollständig verhindert werden kann, so kann doch oft die Wahrscheinlichkeit ihres Eintretens verringert werden. Dementsprechend gehören die meisten Risikomaßnahmen zu dieser Kategorie. Ein einfaches, anschauliches Beispiel dafür ist die erneute Eingabebestätigung beim endgültigen Löschen einer Datei, um die Wahrscheinlichkeit für Datenverlust aufgrund Bedienungsfehlern zu verringern.

Verringern der Auswirkung

Neben der Eintrittswahrscheinlichkeit bestimmt die Auswirkung die Größe des Risikos. Allerdings erfordert es oft andere Maßnahmen, um die Auswirkung zu reduzieren. Deshalb ist es sinnvoll, die Reduzierung eines Risikos mit zwei Kategorien abzubilden. So reduziert z.B. das Tragen von Sicherheitsschuhen und Schutzhelmen in einer Lagerhalle die Auswirkungen herunterfallender Gegenstände, während die sichere Verwahrung des Lagergutes die Wahrscheinlichkeit reduziert.

Übertragen auf andere Stakeholder

Dies ist nur dann sinnvoll, wenn die Stakeholder, auf die man das Risiko abwälzen will, besser dafür geeignet sind, das Risiko zu managen. Der Eintritt des Risikos gefährdet ja nach wie vor den Projekterfolg. Typische Maßnahmen, die zu dieser Kategorie gehören, sind das Abschließen von Versicherungen oder die Vereinbarung von Konventionalstrafen mit Lieferanten.

Teilen mit anderen Stakeholdern

Wenn die Bedrohungen die eigene Risikobereitschaft übersteigen, das Projekt aber dennoch sehr attraktiv ist, dann bietet es sich an, die Gefahren auf mehrere Schultern zu verteilen. Die typische Maßnahme dabei ist die Gründung eines Joint Ventures. Normalerweise geht das Teilen der Bedrohung einher mit dem Teilen der Chancen.

Plan B / Notfallplan / Eventualplan

Die Vorbereitung eines "Plan B" ergänzt alle anderen Maßnahmen, welche die betrachtete Bedrohung nicht vollständig beseitigen können. Typische Anwendung findet der Plan B bei technischen Unsicherheiten. Wenn z.B. ein innovatives Material sich als nicht geeignet erweist, dann greift man auf ein bekanntes Material zurück, dessen Eignung bereits nachgewiesen ist.

Hot-Stand-By

Der Ausfall eines wichtigen Elements kann durch seine Verdoppelung abgesichert werden. D.h. dasselbe Element – z.B. eine zweite Kamera bei Filmaufnahmen – steht betriebsbereit zur Verfügung, um bei Ausfall des ersten Elements sofort an seine Stelle zu treten. Oftmals wird die Kategorie "Hot-Stand-By" entweder unter eine der Kategorien "Plan B" oder "Verringerung der Auswirkungen" einsortiert. Damit die Kategorienliste ihren Zweck als Checkliste für die Risikoverantwortlichen erfüllt, empfehle ich, den Hot-Stand-By eigens als Möglichkeit aufzuführen.

Maßnahmenkategorien für Chancen

Schaffen

So wie man Bedrohungen vermeiden kann, indem man einen anderen Lösungsweg wählt, so kann man auch bewusst Chancen schaffen, indem man die Voraussetzungen für ihr Eintreten herbeiführt.

Ergreifen

Wenn ein Ereignis eintritt, dass positive Auswirkung auf das Projektziel hat, liegt es natürlich nahe, diese Chance zu ergreifen. Dies ist jedoch nicht selbstverständlich. Zunächst ist abzuwägen, welche weiteren Konsequenzen sich daraus ergeben. Möglicherweise sind mit dem Ergreifen der Chance auch Bedrohungen oder sogar direkt negative Effekte verbunden. Deshalb sind auch Maßnahmen der Kategorie "Ablehnen" zu analysieren.

Ablehnen

Eine Chance abzulehnen bedeutet, nicht vom Plan abzuweichen und damit auch nicht die positiven Auswirkungen zu realisieren. Gründe dafür können sein, dass das Ergreifen der Chance auch negative Auswirkungen hat, wie z.B. eine Verzögerung des Liefertermins. Ein weiterer typischer Ablehnungsgrund ist, dass das Realisieren der Chance nicht in die Strategie des Unternehmens passt.

Wahrscheinlichkeit erhöhen

Es ist natürlich im Interesse der Projektbeteiligten, Ereignisse zu fördern, die positive Einflüsse haben. Allerdings sind damit meist auch zusätzliche Aufwände verbunden. So kann z.B. die Wahrscheinlichkeit, dass die Benutzer das Projektergebnis akzeptieren, mit Projektmarketing erhöht werden.

Auswirkung erhöhen

Eine Chance kann nur so viel Nutzen bewirken, wie es die Bedingungen zulassen. Z.B. kann die schnellere Erledigung einer Aufgabe nur dann zu einer Verkürzung der Projektdauer führen, wenn die anderen Arbeiten vorverlegt werden können.

Übertragen auf andere Stakeholder

In Kombination mit dem Ablehnen einer Chance ist stets die Überlegung sinnvoll, ob nicht ein anderer Stakeholder von dieser Chance profitieren könnte. Zwar wird damit kein direkter Nutzen für das aktuelle Projekt erzielt, aber der betroffene Stakeholder wird dadurch dem Projekt ggf. mehr unterstützen.

Teilen mit anderen Stakeholdern

Genügen z.B. die eigenen Mittel nicht, um eine Chance zu realisieren, dann kann man sich mit anderen Stakeholdern zusammenschließen. Im einfachsten Fall ist dies die Aufnahme eines Kredits, dessen Zinsen der Anteil des Kreditgebers am Nutzen der Chance sind.

Schritt 4: Benennen Sie die Risikoverantwortlichen!

Je nachdem, welche Rollen Sie im Risikomanagementsystem definiert haben (siehe Schritt 2), ordnen Sie nun für jedes Risiko den dort benötigten Rollen geeignete Ressourcen zu. Tabelle X führt einige Beispiele dafür auf.

Risiko	Risikoeigentümer	Maßnahmen und Ausführende
Strategieänderung des Vorstands macht Projekt überflüssig	Vorsitzender des Lenkungsausschusses	Projektmanager bricht Projekt ab
Neue Anforderungen führen zu Überschreitung des Projektbudgets	Projektmanager	Lenkungsausschuss beschließt über Genehmigung oder Ablehnung
Der Akku erhitzt sich unter den spezifizierten Betriebsbedingungen zu sehr	Dipl.-Ing. P. Meier	Lieferant muss Design des Akkus verbessern
Wettbewerber bringt Konkurrenzprodukt vor uns auf den Markt	Abteilung Marketing	Lenkungsausschuss beschließt über weiteres Vorgehen

Tabelle 1: Beispiele für Zuweisung von Risikoverantwortlichkeiten (Ausschnitt aus einer Risikoliste)

Schritt 5: Setzen Sie die Maßnahmen um oder planen Sie ihre Umsetzung!

Je nachdem, welche Art von Maßnahmen Sie beschlossen haben, welche Ressourcen Sie dafür benötigen und wie umfangreich diese Maßnahmen sind, können Sie diese sofort wirksam werden lassen oder ihre Umsetzung in den Projektplan aufnehmen.

Das Akzeptieren von Bedrohungen oder das Ablehnen von Chancen sind z.B. Maßnahmenkategorien, die sofort umsetzbar sind. Eintrittswahrscheinlichkeiten oder Auswirkungen zu beeinflussen, erzeugt hingegen meist einen höheren Aufwand.

Es ist deshalb sinnvoll, diesen Schritt nach Möglichkeit in die regulären Planungszyklen zu integrieren, z.B. bei Phasenübergängen oder dem Planen einer neuen Iteration.

Starten Sie wieder bei Schritt 1!

Die Schritte 1 bis 5 des Risikomanagementverfahrens sind als beständig zu durchlaufender Zyklus zu verstehen. Maßnahmen zur Behandlung von Risiken werden – dazu werden sie ja ergriffen – zu einer neuen Risikobewertung führen. Zugleich können sie aber auch selbst neue Risiken bewirken.

Kommunizieren Sie beständig Risiken und Maßnahmen an die Stakeholder!

Alle Stakeholder müssen in das Risikomanagement des Projekts einbezogen werden, da alle Beteiligten spezifische Risiken erkennen können.

Integrieren Sie deshalb die Kommunikation über Risiken und die Maßnahmen zur Risikobehandlung in die Berichterstattung des Projekts, z.B. in Statusberichte. Sorgen Sie darüber hinaus dafür, dass alle Stakeholder Einblick in die für sie relevanten Abschnitte der Risikoliste haben. Wenn Sie mit einem **Project Canvas** arbeiten, dann können Sie dort die Risikomatrix integrieren.

Überprüfen Sie, ob die Risikoliste, die ergriffenen und die geplanten Maßnahmen Ergänzungen oder Änderungen im Kommunikationsplan erforderlich machen. Z.B. wenn dadurch weitere Stakeholder hinzugekommen sind, die über bestimmte Entwicklungen informiert werden müssen.

Ergänzende / ähnliche Methoden

- **Risikoidentifikation, Umfeldanalyse, Stakeholdermanagement** und **Lessons Learned** – ergänzende Methoden für Schritt 1: Identifizieren Sie die Risiken!
- **Risikoanalyse** und **Fehlermöglichkeits- und Einflussanalyse (FMEA)** – ergänzende Methoden für Schritt 2: Analysieren und bewerten Sie die Risiken!
- **Ishikawa-Diagramm** – Methode zur Ursachenanalyse von Risikoereignissen
- **Fehlerbaumanalyse** – Methode zur Ursachenanalyse von Risikoereignissen und zur Bestimmung von Eintrittswahrscheinlichkeiten
- **Szenariotechnik** – Methode zur Analyse von Risikoauswirkungen und Risikomaßnahmen
- **Risikomatrix** – zur Visualisierung der Risikoanalyse und zur Kommunikation der Risikosituation an die Stakeholder

Praxistipps

- Weniger ist meistens mehr. Eine sehr einfach gehaltene, jedem bekannte Risikoliste ist mehr wert als eine ausgefeilte Risikodatenbank, auf die nur der Projektmanager selbst Zugriff hat.
- Vernachlässigen Sie nicht die Standardrisiken des Geschäftslebens: Z.B. können Lieferanten plötzlich ausfallen (Verkauf, Insolvenz usw.), ohne dass dafür Anzeichen erkennbar sind.

- Beachten Sie unbedingt Risiken, deren Eintritt andere Risiken beeinflusst (sog. Klumpenrisiken)!
- Verwechseln Sie schleichenden Funktionszuwachs niemals mit einer Chance!
- Die größte Bedrohung eines Projekts besteht in der Verzögerung des Projektablaufs. Risiken (sowohl Chancen als auch Bedrohungen), die die Projektdauer erhöhen, sind besonders zu beobachten.
- Wenn Sie das hier beschriebene Risikomanagementverfahren im Rahmen eines Projektmanagementsystems einsetzen, müssen Sie das Risikomanagementsystem darauf zuschneiden.

Herkunft

In den Lehrbüchern und Richtlinien für Projektmanagement finden sich zahlreiche Versionen für Risikomanagementverfahren. Das hier beschriebene Verfahren orientiert sich zwar an den im PMBOK® Guide beschriebenen Prozessen für Risikomanagement und dem Risikomanagementverfahren von PRINCE2®. Allerdings weiche ich in einer Reihe von Punkten von diesen Richtlinien ab, um Praxisnähe und logische Konsistenz zu gewährleisten.

Der PMBOK® Guide unterscheidet z.B. bei der Risikoanalyse zwischen qualitativer und quantitativer Analyse. Dies ist in der Praxis nicht klar voneinander zu trennen. Das PRINCE2®-Manual integriert in Schritt 1 die Identifikation des Projektumfelds und die Erstellung des Risikomanagement-Ansatzes. Dies verwirrt den Anwender, da dies nur einmal zu Beginn des Projekts durchgeführt wird, während die Identifikation der Risiken laufend erfolgt. Beide Richtlinien integrieren den hier hervorgehobenen Schritt 4: "Bennen Sie die Risikoverantwortlichen!" in die anderen Prozessschritte. Ich halte es für wichtig, diesen Schritt aufgrund seiner Bedeutung bewusst durchzuführen, damit keine nur rein formelle Zuweisung stattfindet.

Autor

Dr. Georg Angermeier

Erstellt am: 07.04.2019

Risikoidentifikation



Die Risikoidentifikation dient zur Feststellung aller relevanten Bedrohungen für ein Projekt. Die Risiken werden systematisch identifiziert und mit ihren Ereignissen, Ursachen und Einflüssen auf das Projekt dokumentiert. Sie bildet die Basis für die anschließende Risikoanalyse im Prozess des Risikomanagements.

Einsatzmöglichkeiten

- Erfassen von Risiken eines Projekts, eines Programms oder eines Projektportfolios
- Erfassen von Risiken in einer Entscheidungssituation
- Erfassen von Risiken auch außerhalb von Projektsituationen, z.B. in Prozessen oder Organisationen

Vorteile

- Die systematische Vorgehensweise gewährleistet, dass möglichst wenige Risiken übersehen werden und somit frühzeitig Maßnahmen geplant werden können.
- Die vollständige Dokumentation der Risiken erleichtert die anschließende Risikoanalyse.

Grenzen, Risiken, Nachteile

- Die Risikoliste ist ohne anschließende Risikoanalyse wenig aussagefähig und kann dadurch zu Missverständnissen in der Kommunikation führen.

- Der Einsatz der Risikoidentifikation garantiert keine 100%ige Vollständigkeit, es können dennoch überraschende Risiken eintreten.
- Die Durchführung der Risikoidentifikation und die Existenz der Risikoliste kann zu einer subjektiven "Scheinsicherheit" führen, aufgrund derer die ständige Überprüfung der Risikobelastung vernachlässigt wird.

Ergebnisse

- Liste mit Beschreibungen aller identifizierten Projektrisiken (Risikoereignis, Ursache(n), Einflüsse auf Projekt).
- Dokumentation der Annahmen bzw. Szenarien, die erarbeitet wurden.

Voraussetzungen

- In der Organisation bzw. im Projektteam müssen eine offene Risikopolitik und ein Risikobewusstsein etabliert sein.
- Im Projekt ist ein Risikomanagementsystem etabliert mit einem definierten Risikomanagementprozess.

Qualifizierung

Für die Risikoanalyse ist keine spezielle Qualifikation erforderlich. Kenntnisse und Erfahrungen in Projektmanagement bzw. Risikomanagement sind hilfreich. Bei der Durchführung mit Arbeitsgruppen ist Moderationserfahrung empfehlenswert.

Benötigte Informationen

- Basisinformationen über das Projekt: Zieldefinition, Spezifikation Projektgegenstand,
- Liste der Stakeholder; falls vorhanden: Ergebnisse der Stakeholderanalyse
- Bestehende Projektdokumente, z.B.: Projektauftrag, Projektstrukturplan, Pläne, Aufwandsschätzungen
- Informationen über Abhängigkeiten und Restriktionen; falls vorhanden: Ergebnisse einer Umfeldanalyse
- Expertise der Teilnehmenden
- Vorgaben und anzuwendende Richtlinien für das Projektrisikomanagement, soweit vorhanden
- Risikokatalog oder Risikochecklisten, soweit zutreffend und vorhanden
- Lessons Learned aus vergangenen Projekten

Benötigte Hilfsmittel

- Moderationsmaterial sowie Pinnwand, Whiteboard, Flipchart etc.
- Hilfsmittel zur Dokumentation der gefundenen Risiken (z.B. Tabellenkalkulation oder Textverarbeitungsprogramm zum Erstellen der Risikoliste, Mind-Mapping-Programm zum Erstellen einer Risk Map, Kamera zur Dokumentation)

Durchführung

- Schritt 1: Beschaffen Sie alle notwendigen Ausgangsdaten!
- Schritt 2: Planen Sie einen Workshop zur Risikoidentifikation!
- Schritt 3: Führen Sie die Risikoidentifikation durch!
- Schritt 4: Dokumentieren Sie die Ergebnisse!
- Ergänzende / ähnliche Methoden

Die Normen für Risikomanagement und die Richtlinien für Projektmanagement behandeln Risiken als Oberbegriff für Bedrohungen und Chancen. In der Praxis werden jedoch Risiken weiterhin im traditionellen Sinne als unsichere Ereignisse mit negativen Auswirkungen auf das Projekt betrachtet und dementsprechend gemanagt. Die folgende Darstellung beschränkt sich deshalb auf die Identifikation von Bedrohungen.

Schritt 1: Beschaffen Sie alle notwendigen Ausgangsdaten!

Stellen Sie sicher, dass alle relevanten Informationen über das Projekt und die Rahmenbedingungen in Form von Projektdokumenten (z.B. Projektauftrag, Projektstrukturplan, Kostenplan, Ablaufplan, Business Case, Lastenheft etc.) vorliegen. Dazu gehören auch, sofern vorhanden, die Ergebnisse einer Umfeldanalyse oder Stakeholderanalyse.

Stellen Sie mit Unterstützung der zuständigen Stelle (z.B. PMO) Erfahrungswerte bisheriger, ähnlicher Projekte zusammen. Überprüfen Sie, ob es einen Risikokatalog oder Risikochecklisten gibt.

Schritt 2: Planen Sie einen Workshop zur Risikoidentifikation!

Die Risikoidentifikation ist eine beständige Aufgabe für alle Stakeholder. Zu Beginn des Projekts, z.B. nach dem Erstellen der Projektpläne, ist ein eigener Workshop mit den relevanten Beteiligten zur grundlegenden Identifikation der Projektrisiken dringend zu empfehlen. Verwenden Sie zur Planung und Durchführung die Methode "**Workshop**" oder die Methode "**Moderation von Arbeitsgruppen**". Beraumen Sie bei Bedarf weitere Workshops an, z.B. bei Phasenübergängen. Bei der Vorbereitung des Workshops sollten Sie die nachfolgenden Punkte speziell für das Risikomanagement beachten.

Teilnehmende festlegen

Die Identifikation von Projektrisiken ist ein sensibles Thema, das die Teilnehmenden aus unterschiedlichen Perspektiven sehen. Ein Workshop in einer sehr großen Runde (etwa mit Auftraggebern, Stakeholdern und Projektteam) ist daher nicht unbedingt zielführend. Beginnen Sie mit einer kleinen Runde zu Beginn (etwa nur Projektleitung und Kernteam). Dies kann bereits zu sehr aufschlussreichen Erkenntnissen führen. Erweitern Sie anschließend die Risikoidentifikation möglichst auf das gesamte Projektteam. Können weitere Experten zur Identifikation beitragen (etwa aufgrund ihrer Erfahrungen mit ähnlichen Projekten), so kann eine Teilnahme dieser Personen an diesem zweiten Workshop sehr sinnvoll sein. Kriterium für die Auswahl der Teilnehmenden ist die benötigte Fachkompetenz.

Falls die Teilnehmerzahl zu groß wird, setzen Sie mehrere Termine an, um ggf. systematisch nach Risikokategorien vorgehen. Grundsätzlich gilt bei der Risikoidentifikation, besser einen Teilnehmer zu viel als zu wenig einzubeziehen. Damit können sich alle in die Thematik einfinden und haben die Möglichkeit, sich mit dem Thema frühzeitig auseinanderzusetzen – insbesondere dann, wenn sie noch keine Erfahrung mit Risikomanagement besitzen. Binden Sie bewusst durch Fragen alle Beteiligten ein und lassen Sie jede Person zu Wort kommen.

Führungskräfte oder Projektauftraggeber bzw. Fördergeber sollten erst dann über die identifizierten Projektrisiken informiert werden, wenn eine Entscheidungsvorlage mit diesen Informationen erarbeitet wurde. Dieser Personenkreis wird deshalb üblicherweise erst dann einbezogen, wenn die maßgeblichen Risiken des Projekts (anhand einer anschließenden Bewertung der Risiken) feststehen und eine Rücksprache mit dem Management erfolgt ist. Dann können die Entscheider beurteilen, ob das Projekt durchgeführt werden soll und welche Risikomaßnahmen ggf. umzusetzen sind.

Eingesetzte Methoden planen

Für eine erste Betrachtung im Rahmen eines Risikoworkshops ist ein kreatives Vorgehen mit Methoden wie **Brainstorming** oder **Mind Mapping** ideal, da so noch keine Vorgaben in Form von Risikokategorien oder Checklisten die Gedanken einschränken.

Danach hilft ein systematisches Vorgehen sehr, möglichst umfassend alle Informationsquellen im Projekt abzuarbeiten. Hierzu stehen Ihnen z.B. zur Verfügung:

- **Risikokatalog**, Risikochecklisten
- **Stakeholdermanagement** (Schritte 1 und 2)
- **Umfeldanalyse**
- **Kraftfeldanalyse**
- **SWOT-Analyse**
- **Ishikawa-Diagramm**
- **Szenariotechnik** (s.u. Schritt 3)

Die Anzahl und Art der eingesetzten Methoden hängen davon ab, welche Informationen bereits vorliegen, wie komplex das Projekt ist und wie stark die Einflüsse des Projektumfeldes sind. Grundsätzlich gilt hier das Prinzip: weniger ist mehr.

Agenda aufstellen

Entwerfen Sie nun eine der Teilnehmeranzahl und dem Methodeneinsatz angemessene Agenda für den Workshop zur Risikoidentifikation. Lassen Sie sich bei Bedarf von einem erfahrenen Moderator beraten und unterstützen.

Dokumentation definieren

Legen Sie fest, in welcher Form die Ergebnisse dokumentiert werden sollen. Berücksichtigen Sie dabei, dass die identifizierten Risiken anschließend noch analysiert werden sollten. Erkundigen Sie sich, ob es eine Vorlage für eine Risikoliste (=Risikoregister) gibt und machen Sie sich mit ihr vertraut.

Schritt 3: Führen Sie die Risikoidentifikation durch!

Bringen Sie zu Beginn des Workshops alle Anwesenden auf den gleichen Informationsstand, was Ausgangssituation und Projektziel angeht. Beziehen Sie im Workshop alle Teilnehmenden mit ein; stellen Sie Fragen und ermuntern Sie alle zur aktiven Mitarbeit.

Kreative Ansätze zuerst

Bevor sie sich die verschiedenen Quellen vornehmen, die sie für den Workshop vorbereitet haben, gehen Sie kreativ an das Thema heran (Brainstorming, Mind Mapping) und stellen Sie offene Fragen wie etwa:

- Wobei haben wir Bauchschmerzen?
- Was fürchten wir am meisten?
- Was darf auf keinen Fall passieren?

Systematische Arbeit mit Projektdokumenten und Einsatz weiterer Methoden

Je nachdem, welche Informationen Ihnen vorliegen und mit welchen weiteren Methoden Sie beschlossen haben zu arbeiten, gestalten Sie gemäß Ihrer Agenda den weiteren Verlauf des Workshops. Berücksichtigen Sie dabei folgende übergreifenden Punkte:

- Wie komplex ist das Projekt selbst oder seine Organisation - und welche Risiken erwachsen daraus?
- Welche Arbeitspakete liegen auf dem kritischen Weg und welche Risiken resultieren daraus?
- Welche Risiken werden durch Schnittstellen / Lieferanten / Kunden ins Projekt getragen?
- Wie zuverlässig sind die Rahmenbedingungen?
- Auf welchen Annahmen beruhen die Pläne und Szenarien? Sind sie plausibel?
- Hatten die Ersteller von Plänen und Aufwandsschätzungen das erforderliche Knowhow?
- Nutzen Sie das Erfahrungswissen der Teilnehmenden: Was ist in vergangenen ähnlichen Projekten schiefgelaufen?

Szenariotechnik als systematisches Vorgehen

Nutzen Sie Szenarien, die etwa für die Kostenplanung bzw. Aufwandsschätzung bereits als "Worst Case" aufgestellt wurden oder stellen Sie selbst ein derartiges Szenario auf. Beschreiben Sie dazu die Rahmenbedingungen, die eine möglichst negative Umgebung beschreiben. Ist etwa ein neuer Lieferant X im Projekt einbezogen, mit dem es noch keine Erfahrungen gibt bzgl. Zusammenarbeit, so wäre ein mögliches Beispielszenario "Die Zusammenarbeit mit dem Lieferanten X funktioniert nicht":

- Beim Lieferanten X sind die internen Prozesse nicht geklärt.
- Der Lieferant X benennt keinen definierten Ansprechpartner für das Projekt.
- Die Projekttermine (Liefertermine) werden intern nicht abgestimmt.
- Die Aufträge des Projekts werden beim Lieferanten nicht priorisiert.
- Risiken, die sich daraus ableiten lassen:
- Die vereinbarte Lieferzeit wird nicht eingehalten, der Termin des entsprechenden Arbeitspaketes verzögert sich.
- Die Terminverzögerung beim Lieferanten wird nicht ans Projektteam kommuniziert.
- Die angeforderte Qualität wird nicht geliefert.
- Die ggf. notwendigen Nachbesserungen werden nicht priorisiert durchgeführt und führen zu weiteren Verzögerungen

Dokumentieren Sie die Annahmen des Szenarios und die daraus resultierenden negativen Auswirkungen (Risiken).

Einflüsse auf das Projekt

Beschreiben Sie die Einflüsse, die ein Risikoereignis auf das Projekt haben kann. Es geht dabei noch nicht darum, etwaige Schadenshöhen zu bestimmen. Die Einflüsse müssen keineswegs immer finanzieller Natur sein. Stellen Sie sich vor, dass das beschriebene Risikoereignis eintritt und fragen Sie dann systematisch folgende Dimensionen ab:

- Zeit: Welche Aktivitäten dauern länger oder können nicht rechtzeitig beginnen?
- Kosten: Welche Sachschäden entstehen, welche zusätzlichen Arbeitsaufwände werden erforderlich? Führen Sie hier aber noch keine Kostenberechnungen durch – dies geschieht erst in der Risikoanalyse.
- Umfang: Können vereinbarte Leistungen nicht mehr erbracht werden?
- Qualität: Können die Abnahmekriterien noch erfüllt werden? Wie beeinflusst das Risikoereignis die Kundenzufriedenheit?
- Risiko: Bringt das eingetretene Risiko weitere Risiken mit sich?
- Nutzen: Ist das Projekt weiterhin gerechtfertigt, wenn das Risiko eintritt? Ist die Investition in das Projekt weiterhin sinnvoll?

Ursachen identifizieren

Benennen Sie mögliche Ursachen für die Entstehung der erkannten Risiken bzw. deren Auslöser. Hierfür kann das Ishikawa-Diagramm sinnvoll sein. Allerdings sollten Sie den Umfang des Workshops sinnvoll begrenzen. Falls eine aufwendigere Ursachenanalyse sinnvoll sein sollte, definieren Sie dafür eine eigene Aufgabe außerhalb des Workshops.

Lassen Sie verschiedene Meinungen gelten: Wenn Unstimmigkeit über mögliche Risiken herrscht, nehmen Sie dies in die Dokumentation auf und diskutieren Sie diese Punkte zu einem späteren Zeitpunkt.

Schritt 4: Dokumentieren Sie die Ergebnisse!

Fassen Sie das Ergebnis in einer Risikoliste zusammen, die zu jedem Risikoereignis möglichen Ursachen und die Auswirkungen auf das Projekt enthält. Formulieren Sie dabei die Risikoereignisse möglichst klar und verständlich. Achten Sie auf Eindeutigkeit, um Fehlinterpretationen zu vermeiden.

Eine sehr gute Art, die Risikosituation eines Projekts zu visualisieren, ist eine Risikolandkarte (Risk Map, vgl. Bild 1). Oft werden bei der Betrachtung von Risiken Zusammenhänge und Wechselwirkungen erkannt, die in einer Visualisierung dargestellt werden können. Das bietet für die weitere Risikoanalyse die Chance, sich die entstandene Risikolandkarte des Projekts im Kreis der Beteiligten anzusehen und daraus weitere Schlüsse für die Einschätzung der Risiken und ihrer Eintrittswahrscheinlichkeiten abzuleiten.

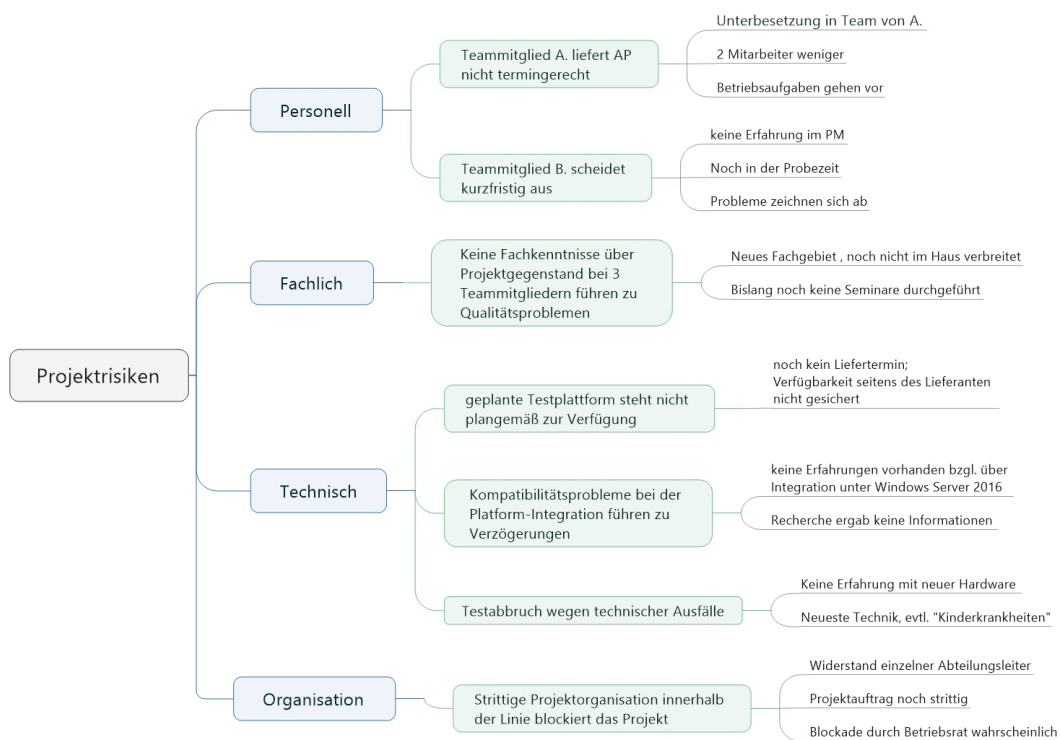


Bild 1: Ausschnitt aus der Risikolandkarte (Risk Map) für ein IT-Projekt, die im Workshop erstellt wurde. Die Risiken sind nach Kategorien (Personell, Fachlich, Technisch, Organisation) geordnet, mögliche Ursachen dazu angegeben.

Ergänzende / ähnliche Methoden

- **Brainstorming** – Kreativitätsmethode zur gemeinsamen Sammlung von Risiken
- **Mind Mapping** – Kreativitäts- und Visualisierungsmethode zur strukturierten Sammlung von Risiken

- **Kraftfeldanalyse** – zur Analyse von Einflussfaktoren
- **Umfeldanalyse** – systematische Betrachtung der Rahmenbedingungen
- **Ishikawa-Diagramm** – Ursachenanalyse und -ermittlung
- **Risikokatalog** – strukturierte Auflistung möglicher Risikoereignisse
- **Stakeholdermanagement** – Betrachtung und Analyse möglicher Stakeholder
- **SWOT-Analyse** – Betrachtung von Risiken und Chancen unter Berücksichtigung von Stärken und Schwächen

Praxistipps

- Schweiften Sie nicht in die Bewertung der Risiken ab, diese ist Aufgabe der Risikoanalyse.
- Falls sich schon mögliche Maßnahmen abzeichnen, notieren Sie diese nur ohne sie zu diskutieren.
- Risikoidentifikation ist eine kreative Aufgabe – gönnen Sie sich deshalb Pausen! Beim Gespräch mit der Kaffeetasse in der Hand eröffnen sich oft neue Perspektiven auf die Dinge.
- Achten Sie darauf, dass der Workshop nicht durch zu viele Methoden überfrachtet wird.
- Formulieren Sie die Risiken eindeutig und unmissverständlich.
- Unterscheiden Sie klar zwischen Risiken und deren Ursachen.

Varianten

Kombination von Risikoidentifikation und Risikoanalyse

Die Identifikation der Risiken wird häufig auch direkt der Risikoanalyse als Bestandteil zugeordnet bzw. beide Methoden werden als eine Einheit gesehen.

Herkunft

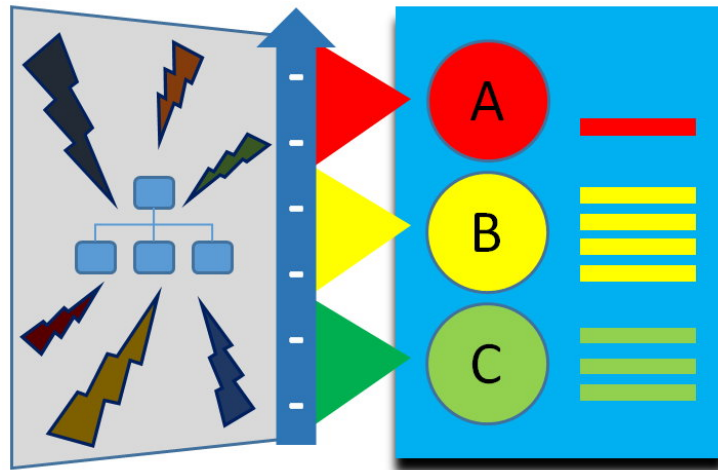
Die Risikoidentifikation ist als Frühwarnsystem zur Erkennung unternehmerischer Risiken ebenso wie zur Erkennung von Projektrisiken etabliert und gilt als grundlegender Bestandteil eines unternehmensweiten Risikomanagementsystems. In den gängigen Standards ist die Risikoidentifikation als Prozessschritt im Risikomanagement von Projekten definiert.

Autorin

Cornelia Niklas

Erstellt am: 22.10.2017

Risikoanalyse



Die Risikoanalyse ist eine Methode zur Untersuchung und Bewertung von Projektrisiken. Deren Gefährlichkeit für den Projekterfolg wird nach Eintrittswahrscheinlichkeit und Größe der Auswirkung eingeschätzt. Die Risiken werden zudem hinsichtlich der zu ergreifenden Maßnahmen priorisiert. Die Ergebnisse werden für die weiteren Schritte im Risikomanagementprozess dokumentiert.

Einsatzmöglichkeiten

- Bewertung der Risikosituation in einem Projekt, Programm oder Portfolio
- Priorisierung der Risiken für weitere Aktivitäten im Risikomanagementprozess
- Prüfung der Durchführbarkeit eines Projekts
- Aufbau eines Risikoportfolios im Programm- und Projektportfoliomanagement

Im Einzelprojekt wird die Risikoanalyse sowohl in frühen Phasen als auch im gesamten Projektverlauf eingesetzt. Die Analyse ist dann auf die Betrachtung von Einzelrisiken innerhalb des Projekts fokussiert. Die Methode ist nicht auf das Projektmanagement beschränkt, sondern kann auch zur Beurteilung von Produkten, Prozessen, Strategien und anderen Geschäftsobjekten eingesetzt werden.

Vorteile

- Die Priorisierung der Risiken gewährleistet, dass die zur Verfügung stehenden Mittel effizient zur Gegensteuerung eingesetzt werden.

- Die Risikosituation und ihre Beurteilung werden dokumentiert und transparent dargestellt, so dass die Stakeholder die Erfolgsaussichten des Projekts verlässlich beurteilen können.
- Die ermittelten Risikokosten liefern eine wichtige Bezugsgröße zur Planung von Maßnahmen.

Grenzen, Risiken, Nachteile

- Eintrittswahrscheinlichkeiten können meist nur ungenau bestimmt werden. Dies stellt in der Praxis die größte Schwierigkeit dar.
- Subjektive Fehleinschätzungen sind auch durch methodisches Vorgehen nicht auszuschließen.
- Der Risiko-Erwartungswert (= Schadenshöhe x Eintrittswahrscheinlichkeit) hat isoliert betrachtet keinen Aussagewert.
- Die Kommunikation der Ergebnisse kann negativ aufgenommen werden, wenn in der Organisation keine offene Risikopolitik herrscht.
- Der Einsatz der Risikoanalyse kann zu unbrauchbaren Ergebnissen führen, wenn kein Risikobewusstsein besteht.

Ergebnisse

- Eintrittswahrscheinlichkeit und Auswirkung (Schadenshöhe) jedes betrachteten Risikos
- Erwartungswert jedes betrachteten Risikos (= Eintrittswahrscheinlichkeit x Schadenshöhe) zur Berechnung der Risikokosten bzw. des Schadensmaßes
- optional: Eintrittsnähe, Wahrscheinlichkeitsdichtefunktionen und Kategorien der Risikoereignisse
- Einteilung der Risiken in Risikoklassen
- Priorisierung der Risiken für die anschließende Risikobehandlung

Voraussetzungen

- Es wurde eine Risikoidentifikation durchgeführt.
- Im Projekt ist ein Risikomanagementsystem etabliert mit einem definierten Risikomanagementprozess.
- In den beteiligten Organisationen sind offene Risikopolitik und Risikobewusstsein vorhanden.

Qualifizierung

Grundkenntnisse in Projektmanagement und Risikomanagement sind erforderlich. Kenntnisse in Statistik (Wahrscheinlichkeitsrechnung) sind hilfreich.

Benötigte Informationen

- Identifizierte und beschriebene Projektrisiken (Risikoliste, Risikolandkarte o.Ä.)
- falls vorhanden: Vorgaben bzw. Richtlinien für das Projektrisikomanagement (z.B. Aussagen über Risikobereitschaft der Projektbeteiligten, Risikokatalog mit standardisierten Maßnahmen)
- falls vorhanden: Definition der Risikoklassen und Bewertungsskalen
- alle bisher erstellten Projektdokumente, insbesondere Pläne

Benötigte Hilfsmittel

- Moderationsmaterial sowie Whiteboard, Flipchart etc.
- Hilfsmittel zur Dokumentation der Ergebnisse (z.B. Programme für Tabellenkalkulation und Textverarbeitung o.Ä.)
- falls vorhanden: Vorlagen, Spezialsoftware für die Risikoanalyse

Durchführung

- Schritt 1: Bereiten Sie den Risikoanalyse-Workshop vor!
- Schritt 2: Besprechen Sie die Skalierung für die Risikobewertung mit den Teilnehmenden!
- Schritt 3: Bewerten Sie die Risiken qualitativ!
- Schritt 4: Priorisieren Sie die Risiken!
- Schritt 5: Führen Sie für Risiken der oberen Risiko-klassen eine genauere quantitative Analyse durch!
- Schritt 6: Dokumentieren Sie das Ergebnis und leiten Sie die weiteren Aktivitäten ab!
- Ergänzende / ähnliche Methoden

Die Normen für Risikomanagement und die Richtlinien für Projektmanagement behandeln Risiken als Oberbegriff für Bedrohungen und Chancen. In der Praxis werden jedoch Risiken weiterhin im traditionellen Sinne als unsichere Ereignisse mit negativen Auswirkungen auf das Projekt betrachtet und dementsprechend gemanagt. Die folgende Darstellung beschränkt sich deshalb auf die Analyse von Bedrohungen.

Schritt 1: Bereiten Sie den Risikoanalyse-Workshop vor!

Beschaffen Sie alle notwendigen Ausgangsdaten. Stellen Sie sicher, dass alle relevanten Informationen vorliegen, die zur Bewertung der Risiken geeignet sind. Hierzu zählen z.B. Erfahrungswerte vergangener Projekte

über Einschätzung von Risiken, Lessons Learned und Rahmenbedingungen. Unbedingt erforderlich sind ferner alle bisher erstellten Projektdokumente wie z.B. Pläne und Spezifikationen, um die Auswirkungen von eingetretenen Risiken beurteilen zu können. Wenn Experten aufgrund ihres Fachwissens und ihrer Erfahrung dazu beitragen können, Risiken besser einzuschätzen, laden Sie diese ebenfalls zum Workshop ein.

Planen Sie die Zeit für den Workshop großzügig, wenn die Teilnehmenden zum ersten Mal eine Risikoanalyse durchführen. Meist entstehen dabei zeitintensive Diskussionen, um die unterschiedlichen Einschätzungen abzugleichen. Haben die Teilnehmenden bereits Erfahrungen mit Risikoanalyse wird meist schneller ein Ergebnis erzielt.

Legen Sie fest, welche Methoden zur Priorisierung der Risiken Sie einsetzen werden. Die Priorisierung kann auf unterschiedliche Weise vorgenommen werden. Verbreitete Methoden sind:

- Priorisierung anhand Eintrittswahrscheinlichkeit und potenzieller Schadenshöhe
- Rangfolge nach Relevanz: Wenn Eintrittswahrscheinlichkeit und Schadenshöhe nicht zur Priorisierung genügen (z.B. große Unsicherheit der Bestimmung), wird die Bedeutsamkeit der Risiken für das Projekt im direkten Vergleich zueinander bestimmt. Die notwendigen Projektaktivitäten werden daraus abgeleitet ohne explizite Gefährdungskategorien bzw. Risikoklassen zu benennen.
- Einteilung in Gefährdungskategorien

Zur Vorbereitung und Durchführung des Workshops können Sie die **Methode Workshop** verwenden.

Schritt 2: Besprechen Sie die Skalierung für die Risikobewertung mit den Teilnehmenden!

Ist bereits ein Standard für die Risikobewertung bzw. -priorisierung vorgegeben, so besprechen Sie mit den Beteiligten kurz, wie die darin beschriebenen Vorgaben (z.B. Skalen für Eintrittswahrscheinlichkeiten und Schadensausmaße) im Einzelnen zu verstehen sind. Meist haben die Personen je nach Tätigkeit und Erfahrung unterschiedliche Vorstellungen davon, was z.B. "Eintrittswahrscheinlichkeit von 25 bis 50%" oder "katastrophaler Schaden" auf das Projekt bezogen genau bedeutet.

Die Eintrittswahrscheinlichkeit

Für die Beurteilung der Risiken nach ihren Eintrittswahrscheinlichkeiten kann eine sehr grobe Skalierung von "gering", "mittel", "hoch" ebenso verwendet werden wie eine detaillierte Skalierung mit Prozentangaben z.B. in 10%-Schritten. Wählen Sie die Skalierung aus, die für Ihre Umgebung am besten geeignet ist und erklären Sie diese anhand konkreter Sachverhalte.

Beispiel:

In einem Unternehmen werden im Jahr ca. 100 Projekte im Kundenauftrag durchgeführt. Im Risikomanagementplan ist festgelegt, dass Eintrittswahrscheinlichkeiten (in Prozenten geschätzt) in eine vierstufige Skala eingeteilt werden:

- selten / unwahrscheinlich: Das Risiko tritt maximal einmal in 25 Projekten ein – entspricht 0-25%.
- gelegentlich: Das Risiko tritt mindestens in jedem vierten Projekt, maximal in der Hälfte aller Projekte ein – entspricht 25-50%.
- häufig: Das Risiko tritt in jedem zweiten Projekt, höchstens in drei Viertel aller Projekte ein – entspricht 50-75%.
- sehr häufig / wahrscheinlich: Das Risiko tritt in mehr als drei Viertel aller Projekte ein – entspricht ca. 75-100%.

Die Schadenshöhe

Für die Einschätzung des Schadens, den ein Risikoereignis im Projekt bewirken kann, wird ebenfalls eine geeignete Stufenskala gewählt. Finanziell quantifizierbare Schäden werden in Geldwerten angegeben. Direkte Auswirkungen auf die inhaltliche Qualität sowie auf den Zeitbedarf des Projekts lassen sich dabei ebenfalls in Geldwerten angeben, etwa durch die Bewertung der daraus entstehenden Folgekosten.

Das Ausmaß ideeller Schäden wird anhand von Beschreibungen im Rahmen dieser Skalierung abgebildet. Am besten werden die Abstufungen wiederum anhand konkreter Sachverhalte beschrieben, wenn keine Vorgaben existieren.

Beispiel

Im Beispielunternehmen bezieht sich die Abstufung für das Schadensmaß auf die im Projekt kalkulierten Gesamtkosten des Projekts. Die Stufeneinteilung für die Schadensmaße in Euro sieht folgendermaßen aus:

- vernachlässigbar: Zusatzkosten unter 5% der Gesamtkosten bzw. vernachlässigbarer ideeller Schaden (ein Kunde ist mit kleinen Unannehmlichkeiten betroffen, aber mit unserer Leistung weiterhin zufrieden)
- erheblich: Zusatzkosten zwischen 5% und 20% der Gesamtkosten bzw. erheblicher ideeller Schaden (ein Stammkunde ist mit wesentlichen Bestandteilen unserer Leistung unzufrieden und beschwert sich, keine Auswirkung auf andere Kunden)
- bedrohlich: Zusatzkosten zwischen 30% und 50% der Gesamtkosten bzw. bedrohlicher ideeller Schaden (ein Konflikt mit einem langjährigen, guten Stammkunden, der eine Eskalation nach sich zieht, Wahrnehmung bei weiteren Kunden)
- katastrophal: Zusatzkosten von mehr als 50% der Gesamtkosten bzw. katastrophaler ideeller Schaden (langjähriger Stammkunde bricht die Zusammenarbeit ab; möglicherweise ein Rechtsstreit als Folge mit Wahrnehmung im Kundenkreis)

Wenn Sie ideelle Schäden benennen, grenzen Sie die Stufen anhand einer klaren Definition der Außenwirkung des Risikoereignisses voneinander ab, um keinen Interpretationsspielraum zu öffnen. Verwenden Sie dazu Szenarien, wenn nötig.

Schritt 3: Bewerten Sie die Risiken qualitativ!

Betrachten Sie die Risiken eines nach dem anderen und schätzen Sie dessen Eintrittswahrscheinlichkeit und

Schadenspotenzial ab. Gehen Sie dabei systematisch vor, z.B. nach verschiedenen Kategorien (wie etwa personell, fachlich, technisch, finanziell, etc.).

- Schätzen Sie, für wie wahrscheinlich Sie den Eintritt des Risikoereignisses halten, wenn nichts dagegen unternommen wird und dokumentieren Sie das Ergebnis in der Risikoliste.
- Schätzen Sie das Schadenspotenzial des Risikos ein, das entweder durch eine direkte Auswirkung auf die Projektkosten oder durch Folgekosten aufgrund einer Verzögerung bzw. Qualitätsverlusten bestimmt ist. Bei ideellen Risiken beschreiben Sie das Schadenszenario, um das mögliche Schadenspotenzial in die Skala einzuordnen.
- Dokumentieren Sie die Ergebnisse in der Risikoliste bzw. der entsprechenden Dokumentation für die Risikoanalyse, um später die Entscheidung über mögliche Maßnahmen zu treffen.
- Fördern Sie dabei die Diskussionen im Team, wenn unterschiedliche Meinungen existieren. Vergleichen Sie die im Laufe des Workshops unsicheren Einschätzungen mit denen bereits bearbeiteter Risiken, um zu realistischen Ergebnissen zu kommen.

Für die Risikoanalyse können Sie je nach Projektgegenstand und Bedarf weitere Methoden verwenden, wie z.B. das **Ishikawa-Diagramm** oder den **Negativen Zweig**.

Weitere Größen, die Sie nach Bedarf bestimmen bzw. abschätzen können sind:

- Eintrittsnähe (Angabe über den frühesten Zeitpunkt, ab dem ein Risiko eintreten kann)
- Wahrscheinlichkeitsdichtefunktionen (erforderlich z.B. für Monte-Carlo-Simulationen)
- Risikokategorie (Clusterung der Risiken anhand eines Risikokatalogs)

Schritt 4: Priorisieren Sie die Risiken!

In diesem Schritt der Risikoanalyse trennen Sie sozusagen "die Spreu vom Weizen": Sie gruppieren die Risiken so, dass klar daraus hervorgeht, worauf das Hauptaugenmerk des Risikomanagements im Projekt gelegt wird. Grundprinzip dabei ist, die Risiken **nach deren Wichtigkeit** zu priorisieren, um daraus eine Abstufung der im Projekt notwendigen Aktivitäten zu erhalten.

Die Priorisierung hängt grundsätzlich davon ab, welche Risikobereitschaft innerhalb der eigenen Organisation vorhanden ist und ob bereits Vorgaben für eine Priorisierung (z.B. im Rahmen eines Risikomanagementplans) gegeben sind.

In der Priorisierung legen Sie fest, für welche "Top"-Risiken mit höchster Priorität ein Maßnahmenplan aufgestellt wird und die Betrachtung und Verfolgung von Indikatoren – sowie die Kommunikation an Projektbeteiligte – stattfinden muss. Ebenso geht daraus hervor, welche Risiken als operative Aufgaben mit mittlerer Priorität im Projekt behandelt werden müssen und welche davon im Moment nicht weiter betrachtet werden. Da die Einschätzung der Risiken nicht mit absoluter Genauigkeit möglich ist, ist eine Feineinteilung der Risiken nach einer exakt berechneten Reihenfolge kaum sinnvoll. Stattdessen ist für die Priorisierung eine Aufteilung der Risiken in Klassen verbreitet.

Bilden von Risikoklassen

Sind Richtlinien vorhanden, die eine Definition von Risikoklassen vorgeben, so verwenden Sie nun diese Vorgaben für die Einteilung der bewerteten Risiken. Falls keine Vorgaben existieren, so können Sie sich an der folgenden Einteilung der Risiken in drei Klassen orientieren:

Klasse 1: projektgefährdende Risiken

Diese Risiken müssen mit oberster Priorität behandelt werden. Klasse 1 erhalten mindestens alle Risiken, die das höchste bzw. zweithöchste Schadenspotenzial bei gleichzeitig hohen Eintrittswahrscheinlichkeiten aufweisen. Im Beispiel wären dies die Risiken der Kombinationen "katastrophal" - "sehr häufig" und "katastrophal" - "häufig" sowie "bedrohlich" - "sehr häufig". Je nach Risikobereitschaft und individueller Stufeneinteilung können weitere Kombinationen dazukommen.

Klasse 2: zu behandelnde Risiken

Darunter fallen Risiken mit relevanter Eintrittswahrscheinlichkeit, die mit Maßnahmen vermieden oder auf ein tolerierbares Restrisiko reduziert werden können. Diese mittlere Klasse erhalten alle Risiken, die ein mittleres oder niedriges Schadenspotenzial besitzen, jedoch niedrigere Eintrittswahrscheinlichkeiten als in Klasse 1. Ein wichtiger Aspekt bei dieser Einteilung ist, dass Risiken mit potenziell extrem hohen Schäden auch dann genauer betrachtet werden müssen, wenn ihre Eintrittswahrscheinlichkeiten sehr gering sind. Denn zumindest muss geprüft werden, ob standardisierte Maßnahmen wie Versicherungen, vertragliche Vereinbarungen etc. dafür im Unternehmensrisikomanagement bereits vorhanden sind (was meistens der Fall ist). Falls nicht, wird abgewogen, ob sich eine weitere Befassung damit lohnt oder nicht – diese Risiken werden im Normalfall jedenfalls nicht automatisch toleriert.

Klasse 3: vernachlässigbare / tolerierbare Risiken

In diese Klasse fallen die Risiken mit geringem bis sehr geringem Schadenspotenzial und niedrigen Eintrittswahrscheinlichkeiten. Diese werden meist unverändert toleriert und erfordern mit Ausnahme der Überwachung keine weiteren Maßnahmen, wenn sich die Einschätzung im Projektverlauf nicht ändert.

Die Klassen 1 und 2 stellen Bedrohungen für das Projekt dar, die im Risikomanagement weiter behandelt werden müssen. Risiken in Klasse 3 werden üblicherweise in Kauf genommen. Sind im Einzelprojekt jedoch sehr viele derart bewertete Risiken vorhanden, sollte aufgrund der damit verbundenen akkumulierten Risikobelastung geprüft werden, wie damit umgegangen werden soll. So kann z.B. untersucht werden, ob gemeinsame Ursachen vorhanden sind oder Abhängigkeiten untereinander existieren. Ggf. sind auch geeignete Maßnahmen zur Reduzierung des Gesamtrisikos erforderlich.)

Schritt 5: Führen Sie für Risiken der oberen Risiko-klassen eine genauere quantitative Analyse durch!

Erarbeiten Sie einen Zahlenwert (d.h., eine numerische Einstufung) zur Bemessung der Risiken. Eine sehr weit verbreitete quantitative Einstufung ist der Erwartungswert des Risikos:

$E = \text{Eintrittswahrscheinlichkeit} \times \text{Schadenspotenzial in Euro}$

Betrachten Sie zum Berechnen des Schadenspotenzials die Folgekosten, die aus Zeitverzögerungen oder Qualitätseinbußen entstehen können. Die Annahmen und Szenarien, die Sie für die Einschätzung der Auswirkungen bei Eintritt des Risikoereignisses aufstellen, gehören zur vollständigen Dokumentation.

Beispiel

Im Beispielunternehmen werden die Folgekosten anhand der Projekterfahrungen geschätzt; z.B. "eine Verzögerung von 3 Monaten kostet uns im Schnitt X Euro" mehr, "eine massive Qualitätsabweichung verursacht durchschnittlich Y Euro an Zusatzkosten". Weitere Folgekosten externer Natur für Dienstleistungen, Rechtsstreitigkeiten oder Gutachter sollten ebenfalls berücksichtigt werden.

Auf Basis der quantitativen Risikoanalyse können im Anschluss die Risikokosten dem Aufwand für Gegenmaßnahmen gegenübergestellt werden, um ein für das Projekt angemessenes Maß zu finden.

Weitere Analysen (für ein gesamtes Risikoportfolio, für die Bewertung von Abhängigkeiten unter Berechnung von bedingten Wahrscheinlichkeiten etc.) erfordern die Anwendung weiterer Simulations- und Prognosemethoden.

Schritt 6: Dokumentieren Sie das Ergebnis und leiten Sie die weiteren Aktivitäten ab!

Als Ergebnis der Risikoanalyse haben Sie nun eine klare Sicht auf die Gefährlichkeit der Projektrisiken und den möglichen Schaden, der – ohne weitere Aktivitäten – dadurch angerichtet werden kann. Die daraus abzuleitenden Aktivitäten sind nicht Bestandteil der Risikoanalyse selbst.

- Dokumentieren Sie die Risikosituation. Fassen Sie die Bedrohungen des Projekts in Klasse 1 und 2 mit prägnanten Bezeichnungen zusammen und stellen sie deren Erwartungswert (Risikopotenzial) dar.
- Stellen Sie eine Risikomatrix auf, wenn dies gefordert ist oder Sie für die Stakeholder als sinnvoll ansehen. Darin werden die bedrohlichen Risiken nach ihrer Positionierung im Koordinatensystem den entsprechenden Klassen zugeordnet (siehe [Methode Risikomatrix](#))
- Kommunizieren Sie die Top-Risiken (etwa im Projektauftrag oder in Form einer Projektsitzung). Zeigt sich eine Hochrisikosituation, stellen Sie die Frage: Ist das Projekt so tatsächlich machbar? Unter welchen Bedingungen besteht Aussicht auf Erfolg? Sind Auftraggeber und Kunde bereit, die Risiken einzugehen?
- Legen Sie die weiteren Schritte im Risikomanagementprozess fest: Benennen Sie eine verantwortliche Person, um einen Maßnahmenplan zu erstellen und vereinbaren Sie die dafür notwendigen Aktivitäten. Setzen Sie eine geeignete Risikoüberwachung auf. Legen Sie bei einer sehr hohen Risikobelastung der Klasse 3 die weitere Vorgehensweise fest. Planen Sie die Neubewertung der Restrisiken nach der Freigabe der Maßnahmen.

Ergänzende / ähnliche Methoden

- **Risikomatrix** – zur Visualisierung der Ergebnisse
- **Risikokatalog** – ergänzende Methode zur Risikoidentifikation, Kategorisierung und Maßnahmenplanung
- **Negativer / Positiver Zweig** – zur Analyse von Auswirkungen
- **Ishikawa-Diagramm** – zur Identifikation von Risikoursachen

Praxistipps

- Gehen Sie möglichst einfach an die Einschätzung der Eintrittswahrscheinlichkeit heran, damit die Teilnehmer nicht überfordert werden. Nehmen sie praktikable Beispiele zu Hilfe (tritt wöchentlich ein, einmal im Monat, einmal im Jahr), um Wahrscheinlichkeiten greifbar zu formulieren.
- Hinterfragen Sie die bereits getroffenen Einschätzungen der Risiken, wenn Sie bei der Betrachtung eines der Risiken das Gefühl haben, Sie müssten "nachjustieren". Vergleichen Sie dann die Ergebnisse und korrigieren Sie diese bei Bedarf.
- Einander beeinflussende Risiken (bedingte Wahrscheinlichkeiten) sind nicht einfach abzubilden. Kennzeichnen Sie Risiken, deren Eintritt möglicherweise von anderen Risiken beeinflusst wird für die spätere Maßnahmenplanung bzw. Risikoüberwachung.
- Seien Sie vorsichtig mit dem Berechnen eines Gesamtrisikos – die Summe der Erwartungswerte ist nur sehr eingeschränkt aussagefähig, da sie keine Abhängigkeiten und bedingten Risiken abbildet.

Varianten

In den Richtlinien und in der Literatur für Projekt- und Risikomanagement werden unterschiedliche Varianten der Risikoanalyse beschrieben hinsichtlich inhaltlichen Umfangs und Abgrenzung der Methoden Risikoidentifikation – Risikoanalyse – Risikobewertung. Die häufigsten Varianten sind:

Integration von Risikoidentifikation und Risikoanalyse

Diese Variante vereint die Risikoanalyse mit der Risikoidentifikation, die nicht als eigene Methode betrachtet wird. Die Identifikation stellt dabei den ersten Schritt der Risikoanalyse dar.

Risiko-Assessment

In dieser Variante wird das methodische Vorgehen in kleinere Einheiten zerlegt: Der Schritt der Risikobewertung / Priorisierung wird als eigene Methode betrachtet und nicht innerhalb der Risikoanalyse durchgeführt.

Bei Informationssicherheits-Risiken wird von einem Risiko-Assessment gesprochen, das aus Risikoidentifikation, Risikoanalyse und Risikobewertung bzw. –priorisierung besteht. Darin ist die Risikoanalyse nur auf die Untersuchung der Auswirkungen und Ursachen beschränkt.

Risikoanalyse im Multiprojektmanagement

In einer Multiprojektumgebung wird durch den Einsatz der Risikoanalyse ein projektweites Risikomanagement unterstützt; im Rahmen einer Risikoportfoliobetrachtung können weitergehende Maßnahmen zur Risikobehandlung auf Basis von Abhängigkeiten und Synergieeffekten zwischen Projekten auf den Weg gebracht werden.

In einer Multiprojektumgebung stößt jedoch die Betrachtung und Einschätzung der Einzelrisiken je Projekt an ihre Grenze, da projektübergreifende Wechselwirkung und Abhängigkeiten nicht berücksichtigt werden können: Die Summe der Einzelrisiken stellt nicht automatisch das Gesamtrisiko des Portfolios dar.

In dieser Situation ist eine projektübergreifende, methodisch unterstützte Risikoaggregation notwendig, um den Gesamtrisikoumfang des Portfolios zu ermitteln.

Herkunft

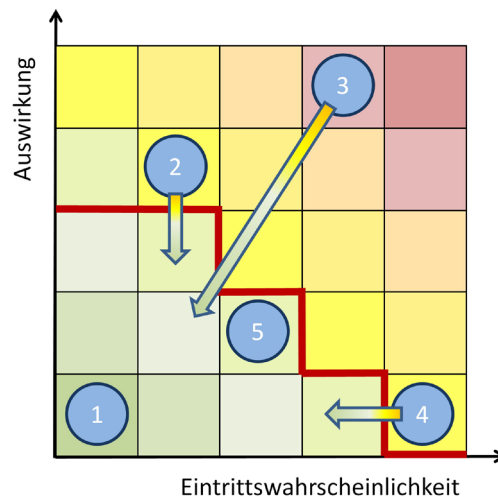
Die Risikoanalyse im Projektmanagement wurde seit den siebziger Jahren vor allem im Rahmen technischer Projekte eingesetzt. Mittlerweile ist sie in allen Normen und Richtlinien für Projektmanagement als fester Bestandteil enthalten. Sie ist in verschiedenen Varianten als Instrument im betriebswirtschaftlichen Kontext ebenso etabliert wie in speziellen Fachbereichen, wo die Vorgehensweisen jeweils in den Normen zu finden sind – von der Funktionalen Sicherheit über Qualitätsmanagement bis hin zur IT-Sicherheit.

Autorin

Cornelia Niklas

Erstellt am: 10.09.2017

Risikomatrix



Die Risikomatrix visualisiert die Risikosituation eines Projekts, Programms oder Portfolios in einer intuitiven Darstellung. Sie behandelt dabei nur die als Bedrohungen klassifizierten Risiken, nicht die Chancen. Die einzelnen Risiken werden in ein durch Eintrittswahrscheinlichkeit und Auswirkung aufgespanntes Koordinatensystem eingetragen. Mit Hilfe der Risikomatrix können diejenigen Risiken identifiziert werden, die am vorrangigsten zu behandeln sind. Der Einsatz einer Risikomatrix ist eine der einfachsten Methoden des Risikomanagements und nur für Vorhaben mit einfacher und überschaubarer Risikobelastung geeignet.

Einsatzmöglichkeiten

- Bewertung der Risikosituation eines Vorhabens
- Präsentation der Risikosituation für Stakeholder
- Identifikation der zu behandelnden Risiken
- Beurteilung der Effizienz von Risikomaßnahmen

Vorteile

- Intuitive Visualisierung der Risikoliste
- Ohne umfangreiche Vorkenntnisse sofort einsetzbar

Grenzen, Risiken, Nachteile

- Die Akkumulation von Risiken wird nicht berücksichtigt.
- Die Wechselwirkungen zwischen Risiken werden vernachlässigt.
- Die Risikomatrix berücksichtigt nur Eintrittswahrscheinlichkeit und Auswirkung, nicht andere Faktoren wie Eintrittsnähe oder die Wahrscheinlichkeit, das Risikoereignis zu erkennen.
- Die Methode ist nur für Vorhaben mit einer geringen Anzahl von Risiken und einer insgesamt niedrigen Risikobelastung geeignet.
- Die intuitive Darstellung verleitet die Anwender dazu, statistische Zusammenhänge zu vernachlässigen.

Ergebnisse

- Flipchart und Stifte
- optional: Tabellenkalkulationssoftware
- optional: Software für Risikomanagement

Voraussetzungen

- Es gibt ein definiertes Risikomanagement-Verfahren, das im Projekt gilt und eingesetzt wird.
- Die Risikobelastung des Projekts ist insgesamt niedrig.
- Auftraggeber und Projektteam sind bereit, Risikomanagement umzusetzen.
- Die Risikoidentifikation wurde durchgeführt und für jedes Risiko ein Verantwortlicher benannt.

Qualifizierung

- Grundkenntnisse des Risikomanagements
- Kenntnisse in Statistik sind hilfreich.

Benötigte Informationen

- Liste der mit Eintrittswahrscheinlichkeit und Auswirkung bewerteten Risiken, die eine Bedrohung darstellen
- Liste der Risikoverantwortlichen

- Anzuwendende Richtlinien für Risikomanagement (z.B. Risikomanagementplan, Risikomanagementstrategie, Risikomanagementsystem)
- Aussage über die Risikobereitschaft der Trägerorganisation

Benötigte Hilfsmittel

- Flipchart und Stifte
- optional: Tabellenkalkulationssoftware
- optional: Software für Risikomanagement

Durchführung

- Schritt 1: Legen Sie die Skalen fest und erstellen Sie die Matrix!
- Schritt 2: Tragen Sie die Risikobereitschaft der Trägerorganisation ein!
- Schritt 3: Tragen Sie die Risiken aus der Risikoliste in die Matrix ein!
- Schritt 4: Identifizieren Sie die zu behandelnden Einzelrisiken!
- Schritt 5: Veranlassen Sie die notwendigen Risikomaßnahmen!
- Schritt 6: Bewerten Sie die Risiken neu!
- Schritt 7: Kommunizieren Sie die Risikosituation des Projekts!

Schritt 1: Legen Sie die Skalen fest und erstellen Sie die Matrix!

Die quantitative Bestimmung von Eintrittswahrscheinlichkeit eines Risikoereignisses und seiner Schadensauswirkung ist nur selten mit hoher Genauigkeit möglich. Für beide Skalen sind deshalb der Genauigkeit ihrer Bestimmung entsprechende Stufen zu wählen.

Prüfen Sie als erstes, ob die anzuwendenden Richtlinien für die quantitative Risikoanalyse Skalen für Eintrittswahrscheinlichkeit und Auswirkung vorgeben. Legen Sie dann die Skalen für die Risikomatrix fest. Diese können höchstens genauso fein sein wie in den Richtlinien vorgeben, ggf. auch gröber.

Beispiel

Der Risikomanagementplan des Beispielprojekts definiert für die Auswirkungen eines Risikos eine Skala in Schritten von 1.000 Euro. Das Projektbudget beträgt 200.000 Euro, das Risikobudget 10.000 Euro. Für die Risikomatrix setzt der Risikomanagementplan eine dreistufige Skala für die Auswirkungen fest: "gering" bedeu-

tet einen Schaden von bis zu 2.000 Euro, "mittel" entspricht einem Schaden zwischen 2.000 und 10.000 Euro, "hoch" sind Schäden über 10.000 Euro. Die Eintrittswahrscheinlichkeit wird bei der Risikobewertung in 10%-Schritten ermittelt. Für die Risikomatrix sind im Risikomanagementplan ebenfalls drei Stufen definiert: "gering" bedeutet eine Eintrittswahrscheinlichkeit von maximal 30%, "mittel" geht von 30% bis 60% und "hoch" sind alle höheren Eintrittswahrscheinlichkeiten. Bild 1 zeigt die Grundversion dieser Risikomatrix.

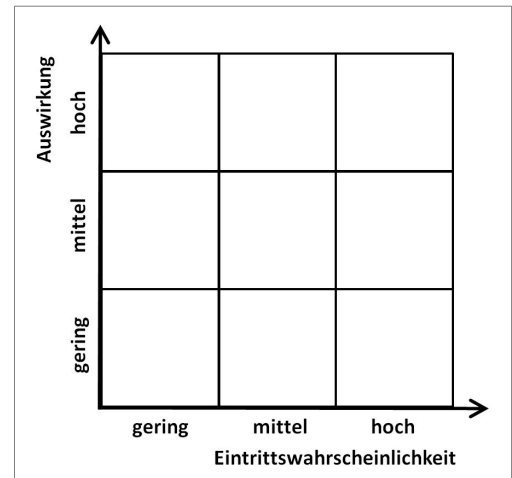


Bild 1: Beispiel für eine 3x3-Risikomatrix.

Schritt 2: Tragen Sie die Risikobereitschaft der Trägerorganisation ein!

Kein Projekt ist vollkommen risikofrei. Aber es ist ein großer Unterschied, ob die Erfolgswahrscheinlichkeit über 90% oder nur bei 66% liegt. Es hängt von der Risikobereitschaft der für das Projekt verantwortlichen Organisation (Trägerorganisation) ab, wie groß die Risikobelastung eines Projekts maximal sein darf. Eine sehr einfache Möglichkeit, die Risikobereitschaft der Trägerorganisation zu visualisieren, besteht darin, in der Risikomatrix eine Grenzlinie einzuzeichnen, unterhalb der alle Einzelrisiken bleiben müssen.

Dabei sind folgende Punkte zu beachten:

- Die Linien gleicher Risikoprioritätszahlen (Produkt aus Eintrittswahrscheinlichkeit und Auswirkung) sind mathematisch gesehen Hyperbeln (siehe Bild 2) und keine Geraden, wie in der Literatur manchmal zu finden ist. Ein Risiko mittlerer Auswirkung und mittlerer Wahrscheinlichkeit ist deshalb wesentlich höher zu bewerten als zwei Risiken geringer Eintrittswahrscheinlichkeit und geringer Auswirkung.
- Zwar addieren sich die Risiken nicht einfach, sondern bilden nach statistischen Gesetzen das Gesamtrisiko, trotzdem kumulieren sich auch viele kleine Risiken zu einer großen Risikobelastung. Es ist deshalb sinnvoll, zusätzlich pro Zelle der Risikomatrix eine Maximalzahl an Risiken festzulegen.

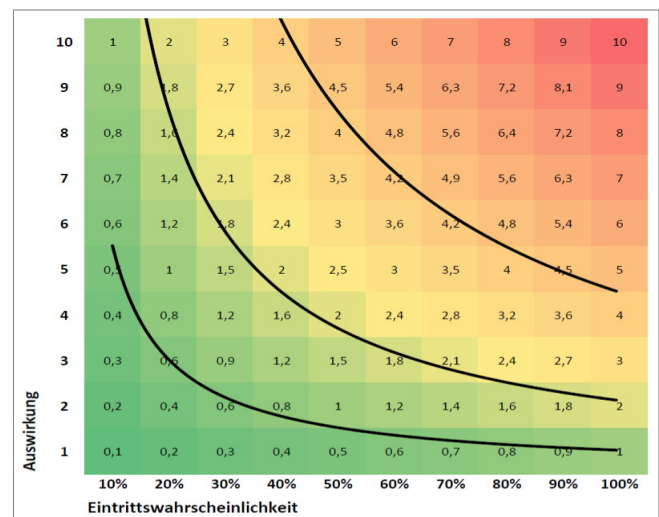


Bild 2: Prinzipieller Verlauf der Risikoprioritätszahlen und möglicher Verlauf von Risikobereitschafts-Linien.

Bei einer 3x3-Matrix ist es also z.B. nicht logisch, die zentrale Zelle als akzeptablen Bereich für Risiken zu bewerten, wenn man nicht auch die rechts und darüber liegenden Zellen akzeptiert. In Bild 3 ist die Risikobereitschafts-Linie so eingetragen, dass nur Risiken akzeptiert werden, die entweder geringe Eintrittswahrscheinlichkeit oder geringe Auswirkung, keinesfalls aber hohe Eintrittswahrscheinlichkeit oder hohe

Auswirkungen haben. Zusätzlich wird im Beispiel festgelegt, dass es maximal je zwei Risiken geben darf, die eine mittlere Eintrittswahrscheinlichkeit oder eine mittlere Auswirkung haben.

Schritt 3: Tragen Sie die Risiken aus der Risikoliste in die Matrix ein!

In den PM-Richtlinien werden gemäß aktueller Normung Risiken allgemein als Unsicherheiten behandelt, die sowohl Bedrohungen als auch Chancen darstellen können. Die Risikomatrix dient nur zur Bearbeitung von Bedrohungen, nicht von Chancen. Falls in der Risikoliste auch die Chancen aufgeführt sind, filtern Sie diese zunächst heraus.

Tragen Sie dann alle verbleibenden, als Bedrohung klassifizierten Risiken in die Zellen der Matrix ein. Dabei bestimmen Eintrittswahrscheinlichkeit und Auswirkung die Koordinaten der zutreffenden Zelle. Sorgen Sie dafür, dass die Symbole in der Matrix dem jeweiligen Risiko zugeordnet werden können, z.B. durch eine eindeutige Nummerierung. Bild 4 zeigt ein beispielhaftes Ergebnis.

Schritt 4: Identifizieren Sie die zu behandelnden Einzelrisiken!

Auf den ersten Blick ist es sehr einfach, die Risiken zu identifizieren, für die geeignete Maßnahmen zu ergreifen sind: Alle Risiken rechts oberhalb der Linie für die Risiko-bereitschaft. Allerdings sind hierbei unbedingt die Richtlinien zu berücksichtigen, die für das Risikomanagement des Projekts gelten. So kann dort z.B. festgelegt sein, dass Risiken ab einer bestimmten Prioritätszahl an das dem Projekt übergeordnete Risikomanagement zu melden sind (z.B. an das übergeordnete Programm).

Beispiel

Der Risikomanagementplan des Beispielprojekts besagt, dass die Klassifizierung identifizierter Risiken durch Reduzierungsmaßnahmen nur um jeweils maximal eine Stufe hinsichtlich Eintrittswahrscheinlichkeit und Auswirkung verbessert werden darf. Damit soll eine zu optimistische oder "politische" Risikobehandlung unterbunden werden.

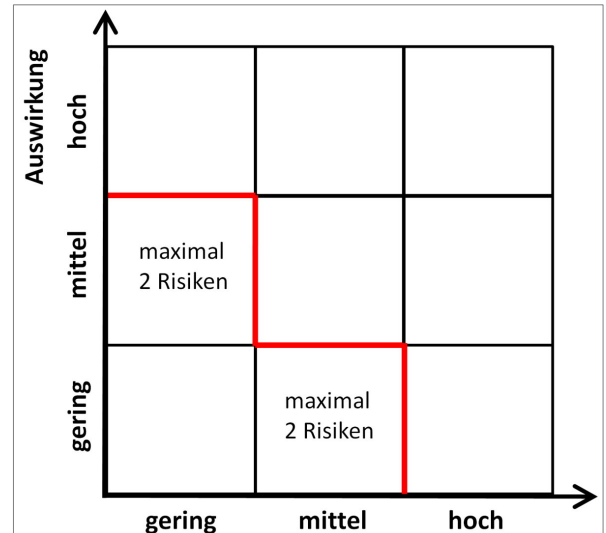


Bild 3: Beispiel einer groben Risikomatrix mit mittlerer Risikobereitschaft.

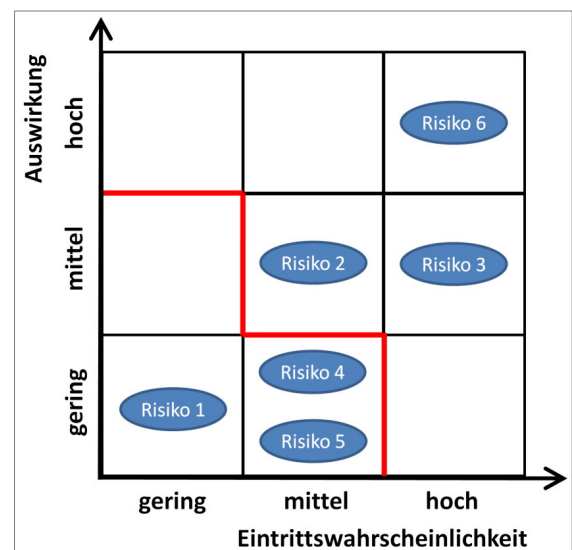


Bild 4: Beispiel einer Risikomatrix mit eingetragenen Risiken

Risiko 6 im Beispiel (siehe Bild 4) kann gemäß Risikomanagementplan gar nicht unter die Linie für die Risikobereitschaft reduziert werden. Die einzige Möglichkeit besteht somit darin, dieses Risiko vollständig zu vermeiden.

Risiko 3 kann im Beispiel nur auf die Zelle mit mittlerer Wahrscheinlichkeit und geringer Auswirkung reduziert werden. Dann sind in dieser Zelle aber drei Risiken. Mindestens eines der dort bereits befindlichen Risiken (Risiko 4 und Risiko 5) müssen somit ebenfalls behandelt werden.

Die Vorgaben für die Behandlungen der Risiken im Beispiel lauten somit:

- Risiko 6: vollständig vermeiden
- Risiko 5: Eintrittswahrscheinlichkeit und Auswirkung um jeweils eine Stufe reduzieren
- Risiko 2: Eintrittswahrscheinlichkeit um eine Stufe reduzieren
- Risiko 4: Eintrittswahrscheinlichkeit um eine Stufe reduzieren

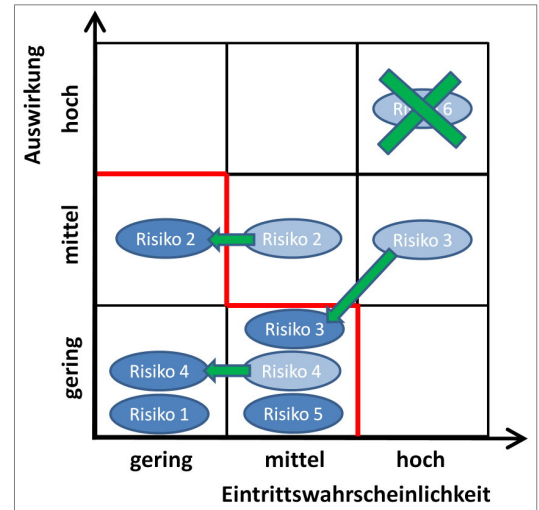


Bild 5: Vorgaben zur Risikobehandlung.

Bild 5 visualisiert diese Vorgaben.

Schritt 5: Veranlassen Sie die notwendigen Risikomaßnahmen!

Informieren Sie die Risikoverantwortlichen der zu behandelnden Risiken und fordern Sie diese dazu auf, gemäß den anzuwendenden Richtlinien die notwendigen Maßnahmen für diese Risiken zu ergreifen. Dies kann weitere Auswirkungen auf die Projektplanung haben, z.B. wenn ein Risiko vollständig vermieden werden muss und deshalb ein anderer Lösungsansatz für eine bestimmte Aufgabe zu finden ist.

Beispiel

Risiko 6 besteht darin, dass ein neues Material die ersten Belastungstests nicht besteht. Da dieses Risiko nicht entsprechend reduziert werden kann, muss auf den Einsatz dieses Materials verzichtet werden. Dies führt dazu, dass auch Spezifikationen und ggf. weitere Dokumente geändert werden müssen.

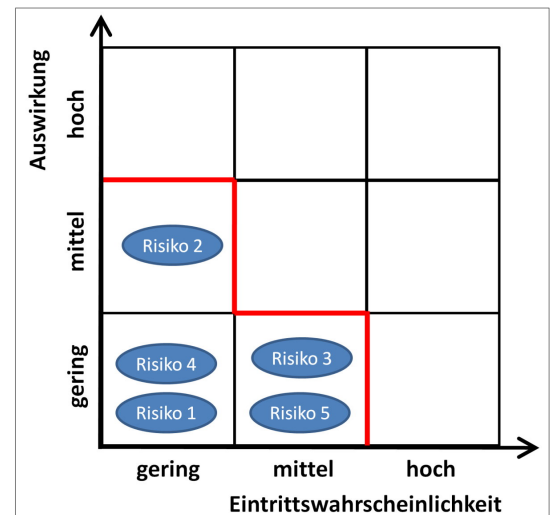


Bild 6: Risikomatrix nach der Durchführung erster Maßnahmen.

Schritt 6: Bewerten Sie die Risiken neu!

Sobald Sie sichergestellt haben, dass alle beschlossenen Risikomaßnahmen ergriffen worden sind, führen Sie eine erneute Risikobewertung durch und tragen diese in die Risikomatrix ein (Bild 6). Beachten Sie, dass unter Umständen neue Risiken hinzugekommen sein können.

Schritt 7: Kommunizieren Sie die Risikosituation des Projekts!

Die Richtlinien für das Risikomanagement sollten definieren, welche Stakeholder über die Risikosituation informiert werden müssen und ob ggf. weitere Entscheidungen notwendig sind. Beachten Sie zudem eventuelle Aussagen des Kommunikationsplans hierzu. Auf jeden Fall sollten Sie dem Lenkungsausschuss die aktuelle Risikobelastung des Projekts anhand der endgültigen Risikomatrix präsentieren, damit dieser diese akzeptieren oder ggf. weitere Maßnahmen veranlassen kann.

Praxistipps

- Wählen Sie die Skalen nicht feiner als eine belastbare Aussage über Eintrittswahrscheinlichkeit und Auswirkung getroffen werden kann.
- Verwenden Sie einen Risikokatalog, in dem auch Standardmaßnahmen und ihr Effekt auf die Behandlung von Risiken dokumentiert sind.
- Legen Sie zusätzlich zur Risikobereitschaftsline auch maximale Anzahlen von Risiken pro Zelle der Matrix fest.
- Überprüfen Sie die Gültigkeit der Risikomatrix in regelmäßigen Abständen, mindestens jedoch zu jedem Projektstatusbericht.

Herkunft

Für die Herkunft der Risikomatrix bzw. die erstmalige Anwendung der Portfoliotechnik auf das Risikomanagement gibt es in der Literatur keine Quelle. Die Risikomatrix / das Risikoportfolio findet sich in nahezu allen Standardwerken zum Thema Risikomanagement.

Autor

Dr. Georg Angermeier

Erstellt am: 10.11.2015

Risikokatalog

Technik	Markt	...
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Material	<input type="checkbox"/> Wettbewerb	<input type="checkbox"/> ...
<input checked="" type="checkbox"/> Fehlfunktion	<input checked="" type="checkbox"/> Kunden	<input type="checkbox"/> ...
<input checked="" type="checkbox"/> Umgebung	<input checked="" type="checkbox"/> Regionen	<input type="checkbox"/> ...
<input type="checkbox"/> ...	<input type="checkbox"/> ...	<input type="checkbox"/>

Ein Risikokatalog listet strukturiert mögliche Risikoereignisse auf, die den Projekterfolg gefährden können. Darüber hinaus kann er weitere Informationen enthalten wie z.B. empfohlene Risikomaßnahmen. Der Risikokatalog dient zum einen als Checkliste für die Risikoanalyse von Projekten, zum anderen als Informationsspeicher für die kontinuierliche Verbesserung des Risikomanagements. Neben Bedrohungen kann ein Risikokatalog auch Chancen auflisten, die den Projekterfolg fördern.

Einsatzmöglichkeiten

- Erstellung von Checklisten für die Risikoanalyse von Vorhaben
- Planung von Risikomaßnahmen
- Beurteilung der Risikobelastung eines Projekts
- Vergleich der Risikobelastungen von mehreren Projekten
- Beurteilung der Erfolgchancen von Projekten
- Sammlung von Erfahrungswerten aus dem Risikomanagement von Projekten

Vorteile

- Beschleunigt erheblich die Durchführung der Risikoanalyse.
- Erhöht die Wahrscheinlichkeit, dass alle Risiken frühzeitig erkannt werden.
- Ermöglicht es, die Risikobelastungen verschiedener Projekte miteinander zu vergleichen.

- Erleichtert die Planung von Risikomaßnahmen.
- Ermöglicht ein vollständiges Bild über die Risikobelastung und die Erfolgschancen eines Projekts.
- Schärft die Aufmerksamkeit der Projektbeteiligten für das Risikomanagement.
- Reduziert die Gefahr, dass sich gleiche Schadensereignisse in aufeinanderfolgenden Projekten wiederholen.

Grenzen, Risiken, Nachteile

- Die Verwendung einer Liste möglicher Risikoereignisse kann bei den Beteiligten den falschen Eindruck hervorrufen, dass es darüber hinaus keine weiteren Risiken gibt.
- Werden zu viele, trivial wirkende Risikoereignisse aufgelistet, kann dies dazu führen, dass die Beteiligten das Risikomanagement nicht mehr ausreichend beachten.

Ergebnisse

- aktualisierter Risikokatalog
- Risikoliste für ein Projekt
- Liste von Risikomaßnahmen für ein Projekt

Voraussetzungen

- Es gibt im Unternehmen eine Organisationseinheit, die Erfahrungswissen projektübergreifend pflegt, z.B. ein PMO.
- Die Organisationseinheit hat einen Risikomanagement-Plan (bzw. Risikomanagementstrategie, Risk Management Framework).
- Es besteht die Bereitschaft, Risiken wahrzunehmen und sie aktiv zu steuern.

Qualifizierung

Das Arbeiten mit einem Risikokatalog erfordert keine besonderen Qualifikationen. Kenntnisse im Risikomanagement sind vorteilhaft.

Benötigte Informationen

- Branchen- und unternehmensspezifische Standards und Richtlinien für Risikomanagement

- Expertenwissen der beteiligten Personen
- Erfahrungswissen aus abgeschlossenen und evtl. noch laufenden Projekten

Benötigte Hilfsmittel

- Tabellenkalkulationssoftware oder Datenbank
- Bei Gruppenarbeit: Moderationsmaterial (Pinnwand, Moderationskarten, Stifte)

Durchführung

- Schritt 1: Legen Sie die Kategorien fest!
- Schritt 2: Legen Sie die Skalen für die Risikobewertung fest!
- Schritt 3: Legen Sie die Anwendungsbereiche fest!
- Schritt 4: Definieren Sie Maßnahmenkategorien!
- Schritt 5: Erstellen Sie die Tabellenstruktur!
- Schritt 6: Tragen Sie die Risikoereignisse ein!
- Schritt 7: Wenden Sie den Risikokatalog an!
- Schritt 8: Pflegen Sie den Risikokatalog!

Die Arbeit mit dem Risikokatalog wird nicht durch einen immer wieder gleich ablaufenden Prozess definiert, vielmehr können die im Folgenden beschriebenen Schritte auch jeweils für sich allein durchgeführt werden.

Schritt 1: Legen Sie die Kategorien fest!

Für ein effizientes Arbeiten mit einer umfangreichen Liste von Risikoereignissen ist es unbedingt erforderlich, diese zu strukturieren. Die Strukturierung ist zugleich ein wesentlicher Bestandteil der Anpassung des Risikokatalogs an das jeweilige Projektumfeld, z.B. die Branche oder die Projektart.

Beginnen Sie zunächst mit nur einer Ebene von Kategorien. Wenn die Anzahl der Risikoereignisse innerhalb einer Kategorie zu hoch wird, können Sie eine zweite Ebene von Unterkategorien definieren. Als Bezeichnungen für die Kategorien finden sich in der Praxis unterschiedliche Begriffe wie z.B. "Risikofeld", "Risikoart", "Risikotyp" oder "Risikobereich". Wenn Sie nicht einfach beim Begriff "Risikokategorie" bleiben wollen, sollten Sie für die oberste Ebene einen Begriff verwenden, der die Allgemeinheit dieser Kategorisierung zum Ausdruck bringt, wie z.B. "Risikofeld".

Grundsätzlich sind drei inhaltliche Ausrichtungen der Kategorisierung möglich: Nach Risikoursache, nach Managementdisziplin oder nach Risikoauswirkung. Eine Kategorisierung nach Risikoauswirkungen, also z.B. "Verzögerung",

"Budgetüberschreitung", "Nichterfüllung des Leistungsumfang" usw. scheint zwar auf den ersten Blick intuitiv, ist aber nicht zu empfehlen, da die meisten Risikoereignisse mehr als eine Auswirkung haben und demgemäß in mehreren Kategorien aufgeführt werden müssten. In einer stark arbeitsteilig spezialisierten Umgebung kann eine Kategorisierung nach Managementdisziplinen bzw. Zuständigkeitsbereichen sinnvoll sein, wie z.B. "Qualitätsmanagement", "Produktion", "Vertrieb" usw. Am weitesten verbreitet und als erster Ansatz zu empfehlen ist die Kategorisierung nach übergeordneten Risikoursachen wie z.B. "Technik", "Finanzierung", "Markt", "Ressourcen" usw. Für das Zusammenstellen der Kategorien kann ein Risikostrukturplan hilfreich sein, wie er beispielhaft in Bild 1 gezeigt wird.

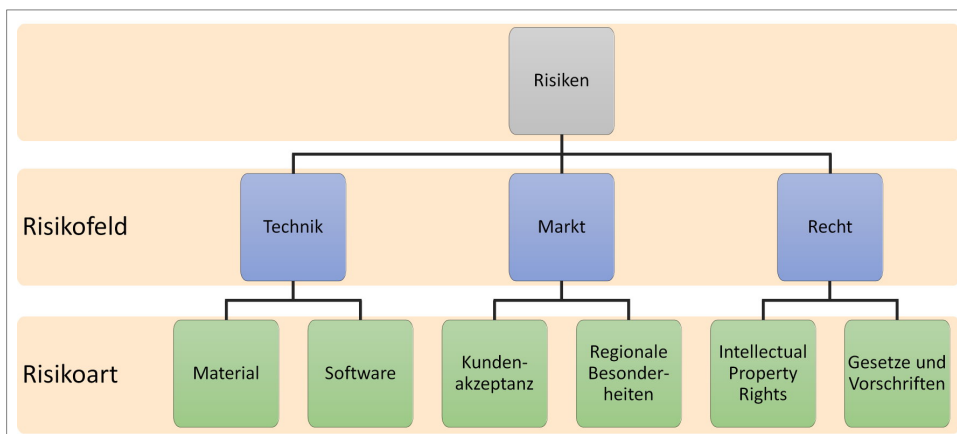


Bild 1: Einfacher Risikostrukturplan mit zweistufiger Kategorisierung (Prinzipiskizze).

Schritt 2: Legen Sie die Skalen für die Risikobewertung fest!

Aus einem Risikoereignis wird ein Risiko, wenn es hinsichtlich Eintrittswahrscheinlichkeit und Auswirkung bewertet wurde. Das Produkt aus diesen beiden Bewertungen dient dazu, die Risiken untereinander zu priorisieren. Allerdings können diese beiden Größen meist nicht exakt ermittelt, sondern nur abgeschätzt werden. Deshalb ist es üblich, hier geeignete Stufenskalen zu definieren, z.B. dreistufige Skalen sowohl für Eintrittswahrscheinlichkeit als auch für die Auswirkung mit den Werten: "gering", "mittel" und "hoch". Aus den möglichen Kombinationen können dann Prioritäten für das Risiko abgeleitet werden. Tabelle 1 zeigt ein Beispiel für die Priorisierung von Risiken, die mit jeweils dreistufigen Skalen für Eintrittswahrscheinlichkeit und Auswirkung bewertet werden.

Eintrittswahrscheinlichkeit	Auswirkung	Risikopriorität
gering	gering	sehr niedrig
gering	mittel	niedrig
mittel	gering	niedrig
gering	hoch	mittel
hoch	gering	mittel
mittel	mittel	hoch
mittel	hoch	sehr hoch
hoch	mittel	sehr hoch
hoch	hoch	extrem

Tabelle 1: Beispiel für eine Risikopriorisierung aus Stufenskalen für Eintrittswahrscheinlichkeit und Auswirkung

Dreistufige Skalen sind einerseits schnell in der Anwendung, andererseits erlauben sie keine feine Differenzierung. Allerdings können zu feine Skalen eine nicht vorhandene Genauigkeit vortäuschen. Ein bewährter Kompromiss sind fünfstufige Skalen.

Für die Übertragung der Skalen auf quantitative Wahrscheinlichkeitswerte oder monetäre Schadenshöhen können keine allgemeingültigen Regeln angegeben werden. Grundsätzlich ist es empfehlenswert, Risiken, deren Eintrittswahrscheinlichkeit einen bestimmten Grenzwert überschreitet (z.B. 60%) nicht mehr als Risiko, sondern als mit Sicherheit eintreffendes Ereignis zu behandeln. Die Möglichkeit, dass dieses Ereignis nicht eintritt, kann dann ggf. als Chance mit einer entsprechend niedrigeren (z.B. 40%) Eintrittswahrscheinlichkeit behandelt werden. Für die Quantifizierung der Auswirkung wird häufig eine nicht lineare, z.T. sogar logarithmische Skalierung verwendet. Dabei steigt die maximale Schadenshöhe pro Stufe z.B. um den Faktor 10 (gering=1.000 Euro, mittel= 10.000 Euro, hoch=100.000 Euro).

Schritt 3: Legen Sie die Anwendungsbereiche fest!

Der entstehende Risikokatalog ist vielfältig einsetzbar, dementsprechend wird er mit der Zeit sehr umfangreich werden. Deshalb sollten Sie bereits frühzeitig die Möglichkeit einplanen, die Einträge nach dem Einsatzbereich zu filtern und so nur relevante Risikoereignisse in der Checkliste für die konkrete Risikoidentifikation zu haben. Für den Einsatz im Projektrisikomanagement sollten Sie z.B. eine Liste der Projektarten definieren, für die der Katalog anzuwenden ist. So sind z.B. für IT-Projekte, Immobilienprojekte, Marketingprojekte oder im Eventmanagement jeweils andere Risiken zu beachten.

Schritt 4: Definieren Sie Maßnahmenkategorien!

Wichtigster Zweck des Risikokatalogs ist letztendlich die Planung von geeigneten Risikomaßnahmen, um die Risikobelastung eines Vorhabens zu reduzieren. Diese sind zwar für jedes konkrete Risiko individuell zu entwickeln, aber für die Risikoverantwortlichen stellt es eine wichtige Unterstützung dar, wenn sie zumindest die möglichen Arten von Risikomaßnahmen für jedes Risikoereignis erhalten.

Übliche Maßnahmenkategorien sind:

- **Vermeiden:** Den Projektplan so ändern, dass das Risikoereignis nicht eintreten kann.
- **Akzeptieren:** Keine aktiven Maßnahmen durchführen, sondern das Risiko nur aktiv überwachen.
- **Auswirkung reduzieren:** Das Projekt vor dem Einfluss durch das Risikoereignis schützen (z.B. stets aktuelle Dokumentation der Projektstätigkeiten, um neue Mitarbeiter schnell einzuarbeiten).
- **Eintrittswahrscheinlichkeit verringern:** Die Ursachen für das Risikoereignis bekämpfen (z.B. Maßnahmen zur Förderung der Gesundheit und Motivation der Mitarbeiter).
- **Notfallplan:** Maßnahmen planen und vorbereiten, die erst bei Eintritt des Risikoereignisses durchgeführt werden, z.B. Backup-Systeme vorhalten.
- **Teilen:** Mit einem Stakeholder vereinbaren, dass die Auswirkungen des Risikos gemeinsam getragen werden.
- **Übertragen:** Das Risiko an einen anderen delegieren, z.B. durch vertragliche Regelungen.
- **Versichern:** Die finanziellen Folgen des Risikoereignisses durch eine Versicherung decken (z.B. Zahlungsausfallsversicherung)#

Beispiel

Für das Risikoereignis "krankheitsbedingter Ausfall von wichtigen Ressourcen" können Risikomaßnahmen der Art "Notfallplan" (z.B. kurzfristiger Einsatz von externen Mitarbeitern) oder "Auswirkung reduzieren" (z.B. ausreichende Pufferzeiten einplanen), nicht aber der Art "Vermeiden" oder "Versichern" eingesetzt werden.

Schritt 5: Erstellen Sie die Tabellenstruktur!

Als nächstes können Sie nun die Tabellenstruktur des Risikokatalogs definieren (bzw. das Datenmodell, wenn Sie mit einer Datenbank arbeiten). Verfolgen Sie dabei das Prinzip "so einfach wie möglich"! Für den Einstieg genügt eine einfache Tabelle mit den vier Spalten: "Risikokategorie", "Risikoereignis", "Erläuterung", "Einsatzgebiete".

Im Laufe der Zeit können Sie dann weitere Spalten hinzufügen, wenn sie sich in der Praxis als hilfreich erweisen. Z.B. kann es sinnvoll sein, für jedes Einsatzgebiet eine eigene Spalte zu definieren, so dass diese separat markiert werden können. Auch kann es sich bewähren, nach Art der Auswirkung (z.B. Zeit, Kosten, Umfang, Qualität, Nutzen, Risiko) zu differenzieren. Schließlich können Sie nach den ersten Erfahrungen Spalten mit empfohlenen Arten von Risikomaßnahmen oder sogar konkreten Risikomaßnahmen ergänzen.

Schritt 6: Tragen Sie die Risikoereignisse ein!

Nun können Sie den Risikokatalog befüllen. Dies kann z.B. im Rahmen eines Projektleiter-Workshops geschehen, in dem diese ihre Erfahrungen mit unerwünschten Abweichungen von Projektplänen zusammentragen. Die Herausforderung dieses Schritts besteht darin, die Einträge im Risikokatalog einerseits so allgemein zu formulieren, dass sie auf andere Projekte übertragbar sind, andererseits dennoch so konkret zu bleiben, dass sie zur Identifizierung der Risiken geeignet sind.

Beispiel

Das konkrete Risikoereignis eines Entwicklungsprojekts: "Im Kippschalter des Staubsaugers kam es durch die beständige mechanische und thermische Belastung zu einem Ermüdungsbruch, so dass sich das Gerät nicht mehr ausschalten lassen konnte, sich dadurch der Motor überhitzte und die Spule durchbrannte." ist für einen Eintrag im Risikokatalog viel zu speziell formuliert. Dagegen kann das davon verallgemeinerte Risikoereignis "Ermüdungsbruch" im Risikofeld "Material" zu abstrakt sein, als dass ein Entwickler damit auch die Gefahr der Fehlfunktion eines Schalters assoziiert. Evtl. kann hier die verallgemeinerte Formulierung "Fehlfunktion von mechanischen Schaltelementen durch Materialversagen" bessere Dienste leisten. Vielleicht ist es auch sinnvoll, aus dieser konkreten Erfahrung mehrere allgemeine Risikoereignisse in den Katalog einzutragen, z.B. "Ermüdungsbruch", "Fehlfunktion von mechanischen Schaltelementen" und "Motorüberhitzung durch Dauerbetrieb".

Schritt 7: Wenden Sie den Risikokatalog an!

Auch wenn der Risikokatalog erst rudimentär erscheint, sollten Sie ihn so schnell wie möglich in der Praxis einsetzen. Nur in der konkreten Anwendung können Sie erfahren, wie der Risikokatalog gestaltet sein muss, um maximalen Nutzen zu entfalten.

Der typischste Anwendungsfall ist die Erstellung einer Checkliste für die Risikoanalyse eines Projekts. Filtern Sie hierzu die Risikoereignisse nach der entsprechenden Projektart und ergänzen Sie die drei Spalten für Eintrittswahrscheinlichkeit, Auswirkung und Risikopriorität. Aus dieser Checkliste erstellen Sie die Risikoliste für das Projekt, indem Sie Schritt für Schritt alle Risikoereignisse betrachten und hinsichtlich ihrer Relevanz für das Projekt analysieren. Gehen Sie dabei folgendermaßen vor:

- Erscheint ein Risikoereignis des Katalogs irrelevant, tragen Sie unter Eintrittswahrscheinlichkeit einfach "0%" ein. Sie haben damit dokumentiert, dass Sie dieses Risiko sehr wohl berücksichtigt haben.
- Erkennen Sie aus dem Risikoereignis genau ein Projektrisiko, dann konkretisieren Sie den Eintrag entsprechend und schätzen Sie Eintrittswahrscheinlichkeit und Auswirkung ab.
- Wenn Sie aus einem Eintrag des Katalogs mehrere Risiken ableiten können, dann lassen Sie den ursprünglichen Eintrag als Überschrift stehen und fügen die einzelnen Risiken darunter in neuen Zeilen ein.
- Überlegen Sie anschließend unbedingt, ob es noch weitere Risiken für Ihr Projekt gibt, die nicht im Risikokatalog aufgeführt sind! Geben Sie diese Risiken an den Eigentümer des Risikokatalogs weiter.

Das weitere Vorgehen mit der so erstellten Risikoliste ist im Risikomanagement-Plan des Projekts geregelt – z.B. die Zuweisung von Risikoverantwortlichen und die Überprüfungsfrequenz.

Schritt 8: Pflegen Sie den Risikokatalog!

Aufgrund der Einzigartigkeit von Projekten entstehen mit jedem neuen Projekt auch neue Risiken. Ein Risikokatalog ist deshalb nur dann nützlich, wenn er kontinuierlich um diese neuen Erkenntnisse und Erfahrungen bereichert wird. Damit dies geschieht, muss eine Person oder Organisationseinheit verantwortlich für die Pflege und Weiterentwicklung des Risikokatalogs sein. Im Idealfall ist es das PMO oder der Riskmanager des Unternehmens. Falls es diese Funktionen nicht gibt, kann z.B. die Qualitätssicherung diese Aufgabe übernehmen. Notfalls führen die Projektmanager individuelle Risikokataloge – in diesem Fall sollten sie aber zumindest im kollegialen Austausch ihre Erfahrungen teilen.

Quellen für die Aktualisierung des Risikokatalogs sind z.B.:

- Risikoanalysen bei Projektplanungen
- Lessons Learned bei Phasenübergängen und Projektabschlüssen
- Projektstatusberichte
- Analysen bei aufgetretenen Fehlern

Praxistipps

- Definieren Sie nicht mehr als zehn Kategorien. Wenn Sie eine feinere Aufteilung benötigen, dann verwenden Sie besser eine zweite Strukturebene.
- Fangen Sie besser schnell mit einem einfachen Risikokatalog an als mit großem Arbeitsaufwand eine anspruchsvolle Erstversion zu erstellen. Die Praxis lehrt am besten, wie der Risikokatalog optimal gestaltet wird.

Varianten

Risikostukturplan

Die einfachste Variante eines Risikokatalogs ist der Risikostukturplan (vgl. Bild 1). Vorteil des Risikostukturplans ist die intuitive hierarchische Darstellung, Nachteil die geringen Möglichkeiten, weitere Informationen darin abzubilden. Für einfache und kleine Projekte kann er ausreichend sein.

Bedrohungs- und Chancenkatalog

Üblich und etabliert ist die Verwendung des Risikokatalogs für Bedrohungen. Wenn im Projekt ein explizites Chancenmanagement eingesetzt werden soll, dann kann er leicht entsprechend erweitert werden. Notwendig ist hier zum einen die Charakterisierung eines Risikos entweder als Bedrohung oder als Chance. Zum anderen gelten für Chancen andere Maßnahmenkategorien, so ist z.B. die Kategorie "Notfallplan" für Chancen nicht sinnvoll.

Mögliche Maßnahmenkategorien für die Behandlung von Chancen sind z.B.:

- **Ablehnen:** Die Chance wird nicht ergriffen, da sie z.B. negative Nebeneffekte wie eine Verzögerung des Markteintritts hätte.
- **Ergreifen:** Falls die Chance eintritt, muss ein Alternativplan vorbereitet sein, mit dem das Projekt die Chance ausnutzt.
- **Eintrittswahrscheinlichkeit erhöhen:** Die Ursachen für das Eintreten der Chance fördern.
- **Auswirkung erhöhen:** Das Projekt so gestalten, dass es die Chance optimal ausnutzen kann.
- **Teilen:** Mit einem Stakeholder vereinbaren, die Chance gemeinsam auszunutzen, z.B. Joint Venture.
- **Übertragen:** Die Chance einem Stakeholder übertragen, ggf. auch für eine Gegenleistung, z.B. Tipp Provision.

Bei Bedarf sind auch die anderen Elemente des Risikomanagements, wie z.B. die Skalendefinitionen für die Behandlung von Chancen anzupassen.

Herkunft

Die Verwendung eines Risikokatalogs ist eine weit verbreitete Methode des Risikomanagements. Eine erstmalige Anwendung oder ein Autor sind nicht bekannt. Das PRINCE2®-Manual enthielt in der Ausgabe 2005 einen einfachen Risikokatalog als Vorlage, die Ausgabe 2009 führt Risikochecklisten und Risikofragebögen nur noch als Instrumentarien für die Risikoidentifikation auf. Der PMBOK® Guide führt neben der Risikocheckliste den Risikostukturplan (Risk Breakdown Structure, RBS) als weiteres Hilfsmittel für die Risikoidentifikation auf. Die Individual Competence Baseline der IPMA (ICB 4.0) fordert lediglich ein "Risk Management Framework", in dem die Methoden und Kategorien für die Risikoidentifikation festgelegt sind.

Autor

Dr. Georg Angermeier
Erstellt am: 17.07.2016

Fehler vermeiden statt aufwendig beseitigen

Mit FMEA auf der sicheren Seite – ein Praxisbeispiel



Dr. Christine Knorr

Dipl.-Physik, selbstständige
Unternehmensberaterin für
technisches Marketing und PM

Vor einiger Zeit bekam ich Post vom Hersteller meiner Spülmaschine. Diese war mit einem Elektronikmodul ausgestattet, auf dem sich ein Bauteil erhitzen konnte. Mindestens zwei Hausbrände waren dadurch bereits entstanden. Bei allen ausgelieferten Spülmaschinen dieser Baureihe musste daher dieses fehlerhafte Modul ausgetauscht werden. Allein bei mir war ein Techniker eine halbe Stunde damit beschäftigt. Welch immenser finanzieller Schaden – nicht zu vergessen der Imageverlust für den renommierten Hersteller – entstanden durch einen Fehler im Design des Produkts! Und dies ist nur ein vergleichsweise "harmloses" Beispiel für eine Vielzahl von Rückrufen, die immer wieder durch die Medien gehen.

Hätte dieser Fehler entdeckt werden können, bevor das Produkt zum Verkauf freigegeben wurde? Im Nachhinein lässt sich das schwer sagen, aber es gibt Methoden, um solche Risiken zu reduzieren. Wie das Beispiel zeigt, ist dies für alle Produkte relevant, nicht nur für sicherheitskritische Anwendungen wie im Automobil oder in der Nukleartechnik. Natürlich steigt die Bedeutung der frühzeitigen Fehlervermeidung mit dem Gefahrenpotential.

Eine bewährte Methode zur frühzeitigen Fehlervermeidung in der Produktentwicklung ist die sog. Fehlermöglichkeits- und Einflussanalyse, kurz FMEA (engl.: Failure Mode and Effect Analysis). Die FMEA zielt darauf ab, potentielle Fehlerquellen für technisches Versagen zu identifizieren und bereits bei Konstruktion und Produktion eines Produkts vorausschauend zu verhindern. Anhand eines leicht verständlichen Beispiels – der sicheren Funktion einer Ampelanlage mit LED-Leuchtmitteln – zeige ich auf, wie FMEA bei Produktentwicklungen die Gefahr von Rückrufaktionen drastisch reduzieren kann. Details (v.a. technische), die für das Verständnis der Methode nicht nötig sind, habe ich vereinfacht und modifiziert.

LEDs statt Glühlampen in Ampelanlagen

Noch bevor die weiße LED den Einzug in die Beleuchtung hielt, wurden lichtstarke, farbige LEDs für den Einsatz in der Signalisierung als Ersatz ineffizienter Glühlampen untersucht. Ein bekanntes Beispiel sind Straßenverkehrssignale – umgangssprachlich "Ampeln" genannt. Neben der Energieeinsparung gegenüber Glühlampen können kostenintensive Wartungsintervalle durch die wesentlich längere Lebensdauer der LEDs ausgedehnt werden.

Neues Produkt muss in bestehender Umgebung zuverlässig funktionieren

Der Einsatz von LEDs statt Glühlampen erforderte jedoch die Entwicklung vollständiger Leuchtmodule – sogenannter LED-Einsätze. Diese LED-Einsätze mussten so beschaffen sein, dass sie in bestehende Ampelgehäuse

montiert werden konnten und elektronisch mit den bestehenden Steuergeräten funktionierten. Anstatt einer Glühlampe mit Sockel, Reflektor und farbiger Streuscheibe waren jetzt LED-Board, Elektronik, Optik, Gehäuse zum Schutz der Elektronik und eine neue Streuscheibe nötig – eine komplette Neuentwicklung (Bild 1).

Vor allem aber war bei dieser Anwendung Sicherheit wichtig. Stellen Sie sich vor, das Steuergerät schaltet auf Rot, der LED-Einsatz leuchtet jedoch aufgrund eines Versagens der Elektronik nicht und das Steuergerät erhält darüber keine Rückmeldung! Die Folge wären Unfälle und Personenschäden, wesnn nicht sogar Todesopfer. Der Ausfall einer Glühlampe war für das Steuergerät leicht zu erkennen, da dann auch der Stromkreis unterbrochen war. Wenn jedoch z.B. die LEDs schneller als erwartet degradierten, dann würde die Elektronik des LED-Einsatzes nach wie vor den gleichen Strom ziehen, obwohl die LEDs selbst nicht mehr ausreichend hell leuchteten.

Wie konstruieren wir Funktionssicherheit?

Dies war die Ausgangssituation eines Entwicklungsprojekts, das ich begleitete. Projektziel waren LED-Einsätze mit High-Power-LEDs für Ampeln. Wir hatten keine Erfahrung mit dieser Anwendung, schließlich handelte es sich um eine Neuentwicklung. Die erste Produktvariante waren LED-Einsätze für Signale mit einem Leuchtfelddurchmesser von 200 mm in rot, gelb und grün. Das Produktkonzept hatten wir bereits fertig ausgearbeitet und erste Muster wurden auf Herz und Nieren getestet.

Doch je näher die Produkteinführung rückte, desto unwohler fühlten wir uns. Uns wurde klar, dass wir zum ersten Mal mit unserem Produkt Menschenleben gefährdeten, wenn es nicht funktionierte – eine ganz andere Situation als beim Ausfall einer LED in einer Schreibtischleuchte. Wir suchten deshalb Rat bei unseren Kollegen aus dem Automobilbereich – dort ist das Thema Produktsicherheit inhärent. Diese empfahlen uns den Einsatz von FMEA.

Was ist die FMEA?

Die FMEA wurde Mitte der 60er Jahre von der NASA für das Apollo-Projekt entwickelt und fand über Luft- und Raumfahrt sowie Nukleartechnik Einzug in viele weitere Branchen. Die FMEA ist eine entwicklungsbegleitende Methode, die vor allem bei neuen Produktkonzepten potentielle Fehler, deren Ursachen und Folgen frühzeitig erkennen kann. Sie wurde zuerst dort eingeführt, wo die Begriffe "Qualität" und "Sicherheit" stark miteinander verknüpft sind. Im Automobilbereich wird die FMEA in der Produktentwicklung zunehmend Pflicht.

Von Konstruktion bis Produktion: FMEA umfasst das ganze Produkt

Die FMEA ist eine induktive Methode, die ausgehend von allen möglichen Fehlern deren Ursachen und Auswirkungen identifiziert und analysiert. Ist der angenommene Fehler z.B. der Ausfall eines Elektronikmoduls, so betrachtet die anschließende Analyse Ereignisse, Prozesse oder Komponenten, die diesen Ausfall verursachen könnten. Dabei geht die Analyse stufenweise bis in die einzelnen Bauteile des betrachteten Produkts und deren mögliche Fehler. Anschließend findet eine Beurteilung statt nach Bedeutung des Fehlers, Wahrscheinlichkeit des Auftretens und Wahrscheinlichkeit des Entdeckens. Je nach Ergebnis werden Abhilfe-Maßnahmen definiert und eingeleitet. Die FMEA ist dabei in den Entwicklungsprozess integriert. Eine interdisziplinäre Zusammenarbeit zwischen den an der Produktentwicklung beteiligten Bereichen ist zwingend notwendig. Eine FMEA wird immer im Team durchgeführt.

Es gibt grundsätzlich zwei Arten der FMEA: Die Produkt-FMEA analysiert das Produktkonzept, die Prozess-FMEA analysiert den Herstellungsprozess. Werden größere Systeme betrachtet, beginnt man die Produkt-FMEA mit einer sogenannten System-FMEA. Diese untersucht in der frühen Entwicklungsphase Systemzusammenhänge des Lösungskonzepts, während die Design-FMEA (auch Konstruktions-FMEA) das geplante Produktkonzept bis in die einzelnen Bauteile und deren funktionale Beziehungen zerlegt.

Fokus auf das Design

Unsere Kollegen aus dem Automobilbereich legten uns nahe, eine Design-FMEA zu starten, da diese mögliche Fehlerursachen bis ins Detail analysiert und hohe Risiken entdeckt und beurteilt, wie z.B. Personenschäden oder hohe Regressforderungen.

Die fünf wichtigsten Merkmale der Design-FMEA sind:

1. Aufdecken von Fehlern und Schwachstellen in einer frühen Phase der Produktentwicklung

Sowohl die Kosten als auch der Zeitaufwand zur Fehlerbeseitigung sind zu Beginn der Produktentwicklung wesentlich geringer als im späteren Prozess oder gar nach Auslieferung (Kosten und Image). In Summe wird die Entwicklungszeit bis zum zuverlässig funktionierenden Produkt verkürzt.

2. Nachweis der Zuverlässigkeit und der Robustheit von Systemen gegenüber Fehlern

Dabei bedeutet Zuverlässigkeit, dass Fehler soweit wie möglich vermieden werden und Robustheit, dass auch im Fehlerfall das System mindestens in einen sicheren Betriebszustand übergeht (z.B. dass die Ampel gelb blinkt).

3. Verifizierung aller im Lastenheft geforderten Merkmale und Funktionen

Ein Fehler ist die Nichterfüllung einer Anforderung. Die Analyse der Fehlermöglichkeiten sichert somit die Erfüllung des Lastenhefts. Bei der Bewertung eines Fehlers wird die Kundensicht herangezogen – Fehlervermeidung steigert deshalb die Kundenzufriedenheit.

4. Aufdecken und Dokumentation systematischer Fehlerzusammenhänge bis auf Bauteilebene

Die Erkenntnisse des FMEA-Prozesses bilden einen großen Wissenspool, der den Mitarbeitern des Unternehmens langfristig für weitere Entwicklungen zur Verfügung steht.

5. Bereichsübergreifende Zusammenarbeit

Der FMEA-Prozess verbessert die Kommunikation und Zusammenarbeit im Unternehmen sowie mit Kunden und Lieferanten.

Der Ablauf einer Design-FMEA wird üblicherweise in fünf Schritte gegliedert:

1. Strukturanalyse des Produkts
2. Funktionsanalyse

3. Fehleranalyse
4. Risikobewertung
5. Maßnahmen zur Optimierung

Start des FMEA-Projekts – warum FMEA?

Wir schlugen unserem Management vor, für das bereits fast fertig entwickelte Produkt eine Design-FMEA durchzuführen. Um die zusätzlichen Kosten und vor allem die zu erwartende Verzögerung zu rechtfertigen, hatten wir zwei starke Argumente: Zum einen führten wir die Reduzierung von Risiken im Betrieb und damit auch die Reduzierung des Produkthaftungsrisikos an. Zum anderen überzeugten wir das Management mit dem Argument, dass wir mit der Methode FMEA einen Wissenspool für die Entwicklung weiterer Produkte in der Signalisierung aufbauen. Diese Erweiterung des Portfolios war Teil der Produktstrategie und wir konnten darlegen, dass der erstmalig hohe Aufwand für die Methode sich später reduzieren würde.

Das FMEA-Team wird definiert und startet

Da wir außer generellem Wissen über die FMEA keine speziellen Kenntnisse hatten, bestanden wir auf einem erfahrenen Kollegen aus der Qualitätsabteilung im Automobilbereich. Dieser sollte unser FMEA-Team in diesem ersten FMEA-Projekt moderieren. Der Projektleiter für die Produktentwicklung des LED-Einsatzes wurde zum Verantwortlichen des FMEA-Projekts ernannt. Als weitere Teammitglieder wurden Vertreter aller Fachbereiche gewählt, die im Produktentwicklungsprozess verantwortliche Rollen besaßen. Dies waren die Bereiche Entwicklung (Mechanik und Elektronik), Messtechnik, Fertigung, Qualität, Produktmanagement und Logistik.

Für die Kernmitglieder aus Entwicklung, Messtechnik, Fertigung und Qualität planten wir zwar eine Weiterbildungsmaßnahme über FMEA ein, allerdings konnten und wollten wir nicht warten, bis ein offizielles Training organisiert war. Um alle Teammitglieder mit ins Boot zu holen, schulte uns der Methodenspezialist aus dem Automobilbereich einen halben Tag.

Unser Moderator startete das FMEA-Projekt mit einer Kick-off-Besprechung. Hauptpunkt war dabei, einen Überblick über alle vorhandenen Unterlagen zu schaffen. Wichtige Unterlagen für das Aufsetzen einer FMEA sind der Terminplan des Entwicklungsprojekts, das Lastenheft, Spezifikationen einzelner Systemelemente, Stücklisten, Testergebnisse, Normen und gesetzl. Vorschriften.

Schritt 1: Die Strukturanalyse des LED-Einsatzes

Bereits beim Kick-off führten wir mit der Strukturanalyse des LED-Einsatzes den ersten Schritt der FMEA durch. Jedes System besteht aus einzelnen Elementen, die das Produktkonzept beschreiben und untergliedern. Ein Strukturbaum ordnet diese Systemelemente in mehreren Strukturebenen hierarchisch an. Die unterste Ebene geht bis in die einzelnen Komponenten des Produkts mit ihren Spezifikationen (z.B. "elektrische Widerstände mit Bauform 0603", "Platine mit Geometrie und Aufbau").

Bild 1 zeigt einen Strukturbaum unseres Produkts. Hier gab es erste Diskussionen: Das LED-Board und die Ansteuerung des LED-Boards waren auf zwei getrennten Platinen untergebracht. Sollten in der ersten Unterstruktur statt des Elements "Elektronik" nicht bereits diese beiden Platinen als zwei einzelne Systemelemente stehen? Beides ist möglich, solange der Strukturbaum vollständig und eindeutig bleibt.

! Es ist wichtig, dass der Strukturbaum das Produkt eindeutig darstellt und jedes Systemelement nur einmal auftaucht.

Systemelemente können auch funktionale Untergruppen eines Bauteiles sein: Die Ansteuerelektronik des LED-Boards befindet sich auf einer Platine, die wir zuerst in einzelne Funktionsblöcke untergliederten (Bild 1). Wir strukturierten die Ansteuerung aber nicht weiter, da sie nach unseren Spezifikationen von einem Lieferanten umgesetzt wurde. Die logische Konsequenz daraus war, dass dieser Lieferant in die FMEA mit eingebunden werden musste (s.u.).

Bei der Strukturierung des Produkts war die vorhandene Stückliste hilfreich, denn diese gab eine mögliche Struktur vor. Die unterste Ebene des Strukturbaums beschreibt die einzelnen Komponenten mit ihren Spezifikationen. In Bild 1 sind für die Komponenten des LED-Boards die Merkmale angedeutet. Z.B. sind die LEDs durch den LED-Typ mit Datenblatt, die festgelegten Helligkeits-, Spannungs- und Wellenlängengruppen, sowie die Lebensdauer spezifiziert.

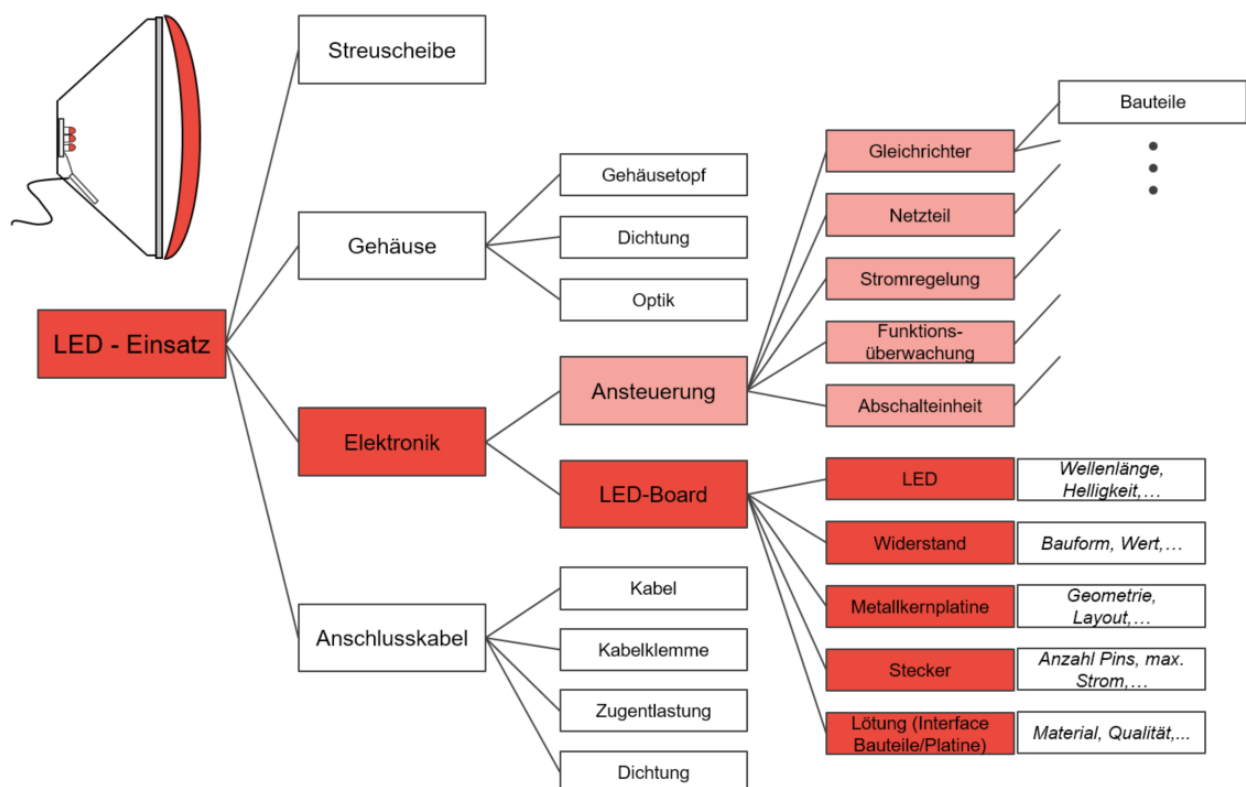


Bild 1: Der LED-Einsatz dargestellt in einem Strukturbaum. Die Merkmale der Komponenten des LED-Boards sind kursiv angedeutet.

Schritt 2: Die Funktionen der Systemelemente analysieren

Jedes einzelne Systemelement besitzt Funktionen oder Aufgaben, die es zu erfüllen hat und benötigt dazu Beiträge anderer Systemelemente. Eine klare Abgrenzung zu Funktionen der unter- und übergeordneten Systemelemente ist bei der Funktionsbeschreibung wichtig. Die Systemstruktur wird im zweiten Schritt der FMEA zu einer Funktionsstruktur aufbereitet, die sehr umfangreich sein kann.

Welchen Umfang und welche Detailtiefe benötigen wir?

Hier stellt sich die grundsätzliche Frage nach dem Umfang der FMEA. Sollen alle Systemelemente betrachtet werden oder eine Auswahl stattfinden? Eine komplette Design-FMEA für ein Produkt ist sehr umfangreich; es werden alle Elemente bis zu den Merkmalen der einzelnen Komponenten auf Fehlfunktionen untersucht. Handelt es sich dabei um eine Produktvariante, die auf einer neuen Plattform basiert, so kann bei einer weiteren Variante auf große Teile dieser FMEA zurückgegriffen werden. Handelt es sich um ein singuläres Produkt oder sind Zeit und Ressourcen knapp, kann es sinnvoll sein, nur die Elemente bzw. Funktionen zu untersuchen, bei denen die größten Herausforderungen bestehen, die dem Kunden am wichtigsten sind oder die Risiken für die Funktionssicherheit beinhalten.

Da wir unser Konzept relativ spät überprüften – erste Freigaben für Serienwerkzeuge waren schon getätigt – wollten wir uns auf die besonders kritischen Elemente und Funktionen fokussieren.

	Streu- scheibe	Gehäuse	Ansteue- rung	LED-Board	Kabel
Lichtstärke in Achse > 200 cd gem. Norm			X	X	
Selbstabschaltung bei < 200 cd (rot)			X	X	
Lichtverteilung gemäß EN 12368, Typ W	X			X	
Phantomlichtklasse mindestens 4	X	X		X	
Lebensdauer 5 Jahre bei 60% Zykluszeit			X	X	

Tabelle 1: Sicherheitskritische Kundenanforderungen und Systemelemente, die im Wesentlichen die Anforderungen umsetzen.

Kritisch sind die neuen Systemelemente Ansteuerung und LED-Board

Tabelle 1 zeigt die sicherheitskritischen Kundenanforderungen an den LED-Einsatz und Systemelemente aus Bild 1. Kreuze geben an, welche Systemelemente die jeweilige Anforderung hauptsächlich umsetzen. LED-Board und Ansteuerung sind damit die wesentlichen sicherheitskritischen Elemente. Zwar waren LEDs keine neue Technologie, aber wir setzten hier ein LED-Board mit High-Power-LEDs zum ersten Mal in dieser Anwen-

derung ein. Auch die Ansteuerung war keine neue Technologie, aber sie wurde ebenfalls in einer neuen Anwendung eingesetzt. Daher beschlossen wir, die Design-FMEA für diese beiden Baugruppen zu starten (rot gekennzeichnete Systemelemente in Bild 1) und wir ließen uns dies vom Management bestätigen.

Die Ansteuerung wurde bei einem Zulieferer entwickelt, der Erfahrung mit sicherheitsrelevanten Schaltungen inkl. Funktionsüberwachung und Abschaltfunktion im Fehlerfall hatte. Dieser Zulieferer war mit FMEA vertraut – der Ursprung der FMEA liegt ja in sicherheitskritischen Anwendungen. Basierend auf unserem gemeinsam erstellten Lastenheft für die Ansteuerung erstellte er eine Design-FMEA, bei der unser Projektleiter mitwirkte. So blieb für uns intern die Fehleranalyse des LED-Boards.

Bild 2 zeigt die Funktionen des LED-Boards, die in der anschließenden Fehleranalyse untersucht werden. Ganz rechts stehen die Merkmale der einzelnen Komponenten, links stehen die Kundenanforderungen an den LED-Einsatz. Die Kundenanforderung "Lichtstärke > 200 cd" (cd=Candela, phys. Einheit) wird z.B. durch die Anforderung an das LED-Board "Lichtstrom > 200 lm" (lm = Lumen, phys. Einheit) und die Funktionen der "Optik" (im Systemelement "Gehäuse") und des Systemelementes "Streuscheibe" erfüllt. Die beiden Elemente "Optik" und "Streuscheibe" beurteilten wir als unkritisch und betrachteten sie in unserer FMEA deshalb nicht. Aus der Anforderung einer maximalen Arbeitstemperatur des LED-Einsatzes von 74°C leiteten wir einen maximal erlaubten Temperaturwert von 80°C am Tc-Punkt des LED-Boards ab.

! Die Funktionen werden am besten im Team zusammengetragen, so erhält man sehr schnell eine vollständige Liste aller Funktionen.

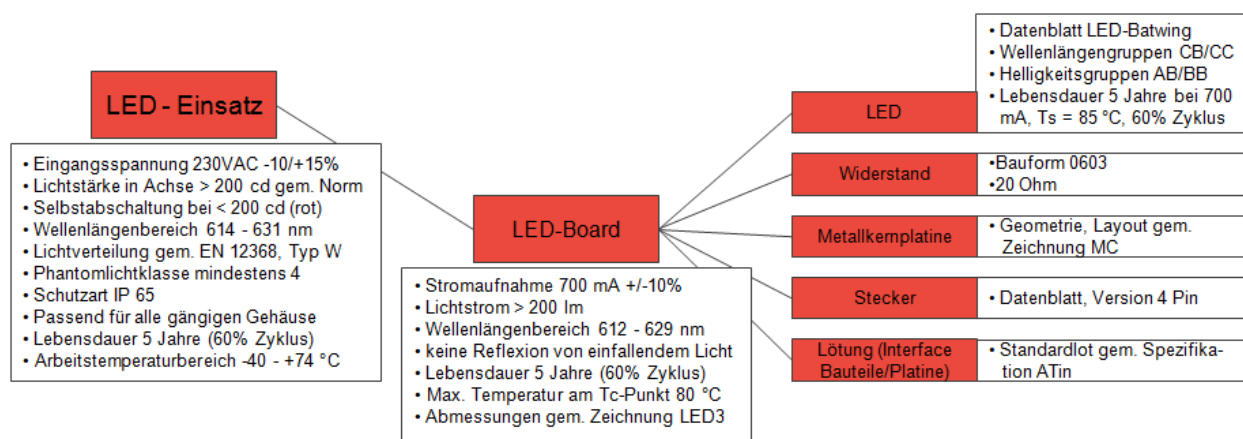


Bild 2: Die Funktionen des LED-Boards mit Merkmalen der Komponenten (rechts) und den Kundenanforderungen des LED-Einsatzes (links)

Schritt 3: Die Analyse potentieller Fehler

Die Ergebnisse der Analysen werden ab diesem Schritt in ein Formblatt eingetragen. Bild 3 zeigt beispielhaft einen Ausschnitt des von uns mit einem Tabellenkalkulationsprogramm erstellten Formblatts. Es ist dabei nicht wichtig, wie und in welcher Reihenfolge die einzelnen Spalten angeordnet werden, sie müssen nur alle vorhanden sein. Wird die FMEA in einem Unternehmen neu eingeführt, ist es sinnvoll, einmal erstellte Vorla-

gen bereichsübergreifend zur Verfügung zu stellen und zu dokumentieren. So kann bei weiteren Entwicklungen einfach auf das Knowhow früherer FMEA-Unterlagen zurückgegriffen werden.

Soll die FMEA großflächig in einem Unternehmen eingeführt werden, kann spezielle FMEA-Software vorteilhaft sein: Diese ermöglicht z.B. einen einfachen Zugriff auf existierende Analysen von immer wieder verwendeten Teilfunktionen oder erlaubt eine Suche nach Fehlerursachen und Fehlerfolgen über Produkte hinweg.

Startpunkt ist die Suche nach potentiellen Fehlern. Zu jeder Funktion des untersuchten Systemelements, hier des LED-Boards, werden alle denkbaren Fehler ermittelt (Spalten "Funktion" und "Fehlfunktion" in Bild 3). Das können sowohl die Nichterfüllung der Funktion als auch Abweichungen davon sein. Anschließend werden die Fehlerfolgen und alle möglichen Fehlerursachen ermittelt (Spalten 4 und 5 in Bild 3).

Beispiel für eine Fehlerkette

Unter der Fehlernummer 2 beschreibt die FMEA-Tabelle (Bild 3) eine der kritischsten Gefahren: Ist der Lichtstrom des LED-Boards zu gering (Fehlfunktion), so ist das Rotsignal nicht mehr erkennbar (Fehlerfolge im LED-Einsatz). Die Fehlfunktion in einem Systemelement verursacht somit die Fehlerfolge des hierarchisch übergeordneten Elements.

Gleichzeitig wird an diesem Beispiel deutlich, dass die Fehlerursache in Fehlfunktionen der untergeordneten Systemelemente liegt: Mögliche Fehlerursachen können eine vorzeitige Alterung der LED oder eine Überhitzung der LED im Betrieb sein (Fehlerursache im untergeordneten Systemelement).

Eine Stromaufnahme außerhalb des vorgegebenen Bereichs (Fehlfunktion) führt zu einer Abschaltung des LED-Einsatzes (Fehlerfolge) mit Rückmeldung zum Steuergerät. Dieser Fehlerfall ist im Design berücksichtigt, das Steuergerät schaltet in den Blinkbetrieb (gelb), bis der defekte LED-Einsatz ausgetauscht wurde.

Fehleridentifikation erfordert Sorgfalt, ist sehr aufwendig und kostet Zeit!

Die Ermittlung aller denkbaren Fehler und deren Ursachen führten wir im Rahmen eines Brainstormings durch. Zusätzlich zu den möglichen Fehlerursachen werden bereits eingeführte Vermeidungs- bzw. Entdeckungsmaßnahmen (VM, EM in Spalte 6, Bild 3) ins Formblatt eingetragen.

Die erstmalige Erstellung der Fehlerliste ist zeitintensiv. Sie muss zwingend im Team durchgeführt werden, denn die Interdisziplinarität ist ein wesentlicher Schlüssel zum Erfolg der FMEA. Oft erkennt man erst während der Diskussion, welche weiteren potentiellen Fehler und vor allem wie viele Fehlerursachen es geben kann.



Ein Trost bei der manchmal stupiden Auflistung möglicher Fehlerursachen ist, dass bei der nächsten Produktvariante viele Fehlfunktionen, Fehlerfolgen und -ursachen in die FMEA-Tabelle übernommen werden können.

Wir erhielten als Ergebnis eine Tabelle, die sich über mehrere DIN A4 Seiten erstreckte. Bild 3 zeigt davon nur einen kleinen Ausschnitt.

FMEA-Art																	
Design-FMEA																	
Produkt		Systemelement		FMEA-Start		Datum der letzten Änderung				Status							
LED-Einsatz 200 mm, rot		LED-Board, rot		28.01.2020		28.02.2020				In Bearbeitung							
Projektverantwortung		Verantwortlicher Fachbereich		FMEA-Teammitglieder										Bearbeiter			
Hans Huber		Produktentwicklung		Maier, Meier, Mayr, Mayer, Meyer, Mair										Mayr			
Nr.	Funktionen	Fehlfunktion	Fehlerfolge	Fehlerursache	Vermeidungs-, Entdeckungsmaßnahmen VM/EM	A	B	E	RPZ	empfohlene Maßnahmen	Verantwortung, Datum, Ziele	getroffene Maßnahmen	A	B	E	RPZ	Status
1	Stromaufnahme 700 mA +/-10%	Stromaufnahme größer/kleiner	Abschaltfunktion der Ansteuerung spricht an; Fehler tritt bei Inbetriebnahme auf	Widerstand zur Strommessung falsch dimensioniert	VM: Aufbau/Test der Schaltung vor Freigabe EM: 100% Ausgangstest am LED-Einsatz	1	7	1	7								
				Layoutfehler	VM: Aufbau/Test der Schaltung vor Freigabe EM: 100% Ausgangstest beim LED-Retrofit	1	7	1	7								
				Abschaltfunktion der Ansteuerung spricht an; Fehler tritt im Betrieb auf	LED defekt innerhalb Lebensdauer	VM: Strom nicht im Grenzbereich; longlife-LED EM:	3	4	10	120							
			2	Lichtstrom > 200 lm während Lebensdauer	Lichtstrom < 200 lm	Rotsignal zu dunkel (< 200 cd in Achse) bei Inbetriebnahme	falsche LED- Helligkeitsgruppe gewählt	VM: Abschätzung mit LED- Datenblattwerten EM: 100% Ausgangstest am LED-Einsatz	3	10	1	30					
Widerstand falsch dimensioniert, dadurch zu geringe Stromaufnahme	VM: Aufbau/Test der Schaltung vor Freigabe EM: 100% Ausgangstest am LED-Einsatz	1	10				1	10									
Rotsignal zu dunkel (< 200 cd in Achse) im Betrieb	LED innerhalb Lebensdauer degradiert (ohne Änderung der el. Eigenschaften)	VM: LED-Strom nicht im Grenzbereich; longlife-LED EM: beschleunigte Lebensdauerests an LED-Boards	4			10	10	400	höhere LED- Helligkeitsgruppen einsetzen Optischen Sensor im LED-Einsatz verwenden	Huber: Klärung der Verfügbarkeit in 2 Wochen Maier: Konzeptvorschläge in 2 Monaten	neue Gruppen, Dokumentation geändert Konzept 1 wird umgesetzt	2	10	10	200	erl.	
	Temperatur am Referenzpunkt > 80°C; dadurch niedrigere LED- Helligkeit	VM: Simulation der Wärmeleitung LED- Board/LED-Einsatz EM: Temperatur- messung im LED- Einsatz	3			10	2	60									
3	Wellenlängenbe- reich 612 - 629 nm	Wellenlänge ausserhalb des spezif. Bereichs	Signal leuchtet außerhalb Normbereich	falsche LED-Wellen- längengruppe	VM: Gruppen mit Normbereich abstimmen EM: Testmessung am LED-Einsatz	1	9	2	18								
				Wellenlänge verschiebt sich durch Strom und Temperatur	VM: EM:	4	9	10	360	Gruppenauswahl unter Berücksichtigung von Strom und Temperatur	Meier, in 2 Wochen	neue Gruppen, Dokumentation geändert	1	9	10	90	erl.
4	keine Reflexion von einfallendem Licht	Reflexion von einfallendem Licht an LED-Board	Signal leuchtet rot, obwohl aus	Reflexion von einfallendem Licht an LED	VM: EM: Phantomlicht- messung am LED- Einsatz	4	4	1	16								
				Reflexion von einfallendem Licht an Platine	VM: schwarze Platinenoberfläche EM: Phantomlicht- messung am LED- Einsatz	2	4	1	8								
5	max. Temperatur am Referenzpunkt 80 °C	Temperatur am Referenzpunkt > 80 °C	LED degradieren schneller	Platinenunterseite uneben; schlechte Wärmeableitung zum Gehäuse	VM: Einkerbung an Nutzen-Trennstellen verhindern Grate EM: Temperatur- messung an LED- Board im Gehäuse	3	10	3	90								
					LED-Pads zu klein	VM: Pads gemäß Datenblattvorgabe EM: Temperatur- messung an LED- Board im Gehäuse	1	10	2	20							
				schlechte Wärmeleitung von LED zur Platine	VM: passendes Lot und geeignete Menge ausgewählt EM: Testmessung an mehreren LED- Boards	2	10	3	60								

Bild 3: Ausschnitt eines Formblatts für Design-FMEA

Schritt 4: die Risikobewertung

Das Risiko bei der FMEA wird mit Hilfe von drei Kennzahlen bewertet:

6. B: Bedeutung der Fehlerfolge aus Kundensicht
7. A: Auftretenswahrscheinlichkeit eines Fehlers mit einer bestimmten Fehlerursache
8. E: Entdeckungswahrscheinlichkeit eines Fehlers mit einer bestimmten Fehlerursache

Jede Kennzahl wird mit einer zehnstufigen Skala von 1 bis 10 Punkten bewertet. Diese drei Zahlen ergeben miteinander multipliziert die sogenannte "Risikoprioritätszahl" (RPZ) mit dem Wertebereich 1 bis 1000. Wir verwendeten für die Bewertung Tabelle 2 als Leitfaden. Sie ist an ein Schema der Automobilindustrie angelehnt. Es gibt auch Bewertungstabellen, die im Detail anders beschrieben sind als Tabelle 2. Wichtig ist, dass Sie während eines FMEA-Projekts immer konsistent zur einmal gewählten Tabelle bewerten.

Die Risikobewertung besteht darin, nacheinander für alle Fehlfunktionen (Spalte 8, Bild 3) die Kennzahlen B, A und E zu bestimmen und daraus die RPZ zu ermitteln.

Wert der Kennzahl	Bewertungskriterien für die Bedeutung "B"	Bewertungskriterien für die Auftretenswahrscheinlichkeit "A"	Bewertungskriterien für die Entdeckungswahrscheinlichkeit "E"
10, 9	Äußerst schwerwiegender Fehler, der die Sicherheit beeinträchtigt und / oder gesetzl. Vorschriften verletzt; existenzbedrohendes Firmenrisiko	Neuentwicklung ohne Erfahrung bzw. unter ungeklärten Einsatzbedingungen; bekanntes System mit Problemen; sehr häufiges Auftreten der Fehlerursache	Sehr geringe Entdeckungswahrscheinlichkeit, da kein Nachweisverfahren bekannt bzw. festgelegt ist
7, 8	Schwerer Fehler mit Verärgerung beim Kunden; Sicherheit ist nicht beeinträchtigt.	Neuentwicklung unter Einsatz neuer Technologien bzw. Einsatz bisher problematischer Technologien; bekanntes System mit Problemen; Fehlerursache tritt wiederholt auf	Geringe Entdeckungswahrscheinlichkeit der Fehlfunktion, da Nachweisverfahren unsicher ist bzw. keine Erfahrung mit dem Nachweisverfahren vorliegt
4, 5, 6	Mittelschwerer Fehler, der beim Kunden Unzufriedenheit auslöst. Kunde nimmt den Fehler war.	Neuentwicklung mit Erfahrung früherer Entwicklungen unter vergleichbaren Einsatzbedingungen; bewährte(s) System / Komponenten mit langjähriger schadensfreier Serienerfahrung unter geänderten Einsatzbedingungen; gelegentlich auftretende Fehlerursache	Mäßige Entdeckungswahrscheinlichkeit der Fehlfunktion; bewährtes Nachweisverfahren aus vergleichbaren Produkten unter neuen Einsatzbedingungen
2, 3	Geringe Funktionsbeeinträchtigung; der Kunde wird nur geringfügig belästigt.	Neuentwicklung mit positiv abgeschlossenem Nachweisverfahren; Detailänderung an bewährtem System mit langjähriger schadensfreier Serienerfahrung unter vergleichbaren Einsatzbedingungen; Auftreten der Fehlerursache ist gering	Hohe Entdeckungswahrscheinlichkeit der Fehlfunktion durch bewährtes Nachweisverfahren; die Wirksamkeit des Nachweisverfahrens wurde nachgewiesen

1	Sehr geringe Funktionsbeeinträchtigung; nur vom Fachpersonal erkennbar	Auftreten der Fehlerursache ist unwahrscheinlich	Sehr hohe Entdeckungswahrscheinlichkeit durch bewährtes Nachweisverfahren und Vorgängergeneration; Wirksamkeit der Entdeckungsmaßnahme für dieses Produkt wurde nachgewiesen
---	--	--	--

Tabelle 2: Bewertungsschema für die drei Kennzahlen, angelehnt an VDA Band 4, Kapitel 3, Produkt- und Prozess-FMEA (VDA, 2006).

Bedeutung "B" der Fehlerfolge

Die Kennzahl "B" gibt an, welche Auswirkungen die Fehlfunktion für den Endkunden hat. Der höchste Wert 10 muss vergeben werden, wenn ein Sicherheitsrisiko eintritt, die Existenz der Firma in Frage stehen kann oder gesetzliche Vorschriften verletzt werden. Eine 1 steht bei sehr geringen Funktionsbeeinträchtigungen, die für den Kunden kaum erkennbar sind.

Klarer Fall: Rotlicht leuchtet nicht oder Gefahr der Produkthaftung

Einfach zu bewerten sind die Extremfälle. So erhielt z.B. die Fehlfunktion "Lichtstrom < 200 lm" zweifelsfrei die Bedeutung 10, da das Rotsignal dann schwerer oder gar nicht erkennbar ist und Unfälle mit Personenschäden geschehen können.

Ähnlich verhielt es sich mit der Fehlfunktion "Wellenlänge außerhalb des spezifizierten Bereichs". Dies hat zwar vermutlich keine Auswirkungen auf den Straßenverkehr, da der Farbunterschied kaum erkennbar ist. Allerdings werden nach Unfällen häufig Signale vermessen. Obwohl es unwahrscheinlich ist, dass rotes Licht, welches nur leicht außerhalb des Normbereiches liegt zu Unfällen führt, könnte dies dennoch zu Regressforderungen führen. Wir wählten daher die 9.

Schwierige Bewertung im Mittelfeld

Während eine extreme Bedeutung klar erkennbar ist, kann man sich im mittleren Bereich oft nur schwer auf eine Bewertung einigen. Ist das eine 4 oder vielleicht doch schon eine 7?

Bei der Fehlfunktion "Stromaufnahme größer / kleiner" diskutierten wir dementsprechend sehr lange: Die Ansteuerung des LED-Einsatzes erkennt diese Fehlfunktion und schaltet den Einsatz ab, das Ampel-Steuergerät erkennt dies und schaltet in den Gelb-Blinkbetrieb. Es gibt kein Sicherheitsrisiko und gesetzliche Forderungen werden zu jeder Zeit erfüllt.

Allerdings muss der Kunde das Signal austauschen und ist vermutlich unzufrieden. Wir wählten schließlich die 7 für den Fall, dass der Fehler schon bei Installation auftritt, hier hat der Kunde ja einen defekten LED-Einsatz erhalten. Tritt der Fehler während des Betriebs auf, wählten wir die 4, da das Eintreten zwar den Kunden verärgert, aber der Fehlerfall nach Lastenheft spezifiziert war.

Auftretenswahrscheinlichkeit "A" eines Fehlers

Die Auftretenswahrscheinlichkeit bewertet die Häufigkeit, mit der die Fehlerursache auftritt und zwar unter Berücksichtigung aller bereits geplanten Vermeidungsmaßnahmen. Eine 10 wird vergeben, wenn die Fehlerursache nahezu sicher auftritt. Eine 1 wird vergeben, wenn es unwahrscheinlich ist, dass die Fehlerursache eintritt (s. Spalte 3 in Tabelle 2).

Hier benötigten wir die Unterstützung unseres FMEA-Moderators in besonderem Maß. Sehr hohe bzw. sehr niedrige Auftretenswahrscheinlichkeiten können in der Regel eindeutig identifiziert werden. Im mittleren Bereich (3 bis 7) ist die Bewertung nicht einfach. Dabei ist es vor allem wichtig, die Bewertung verschiedener Fehlerursachen relativ zueinander stimmig zu halten: Unser Moderator hinterfragte unsere Einschätzung bei jeder Fehlerursache und verglich sie mit bereits erfolgten Bewertungen, bis wir alle einig waren, dass der neue Wert zu allen anderen Bewertungen richtig in Beziehung steht.

Bei besonders strittigen Fehlerursachen ist es hilfreich, einen Blick auf die Bedeutung und die Entdeckungswahrscheinlichkeit zu werfen: Sind beide sehr niedrig bewertet, kann eine endlose Diskussion mit einer ungefähren Bewertung der Auftretenswahrscheinlichkeit beendet werden. Für die weiteren Schritte ist es dann nämlich unerheblich, ob es sich z.B. um eine 5 oder 6 handelt.

Viele potentielle Fehler unseres LED-Boards hatten eine geringe Auftretenswahrscheinlichkeit, da sie mit bereits definierten Vermeidungsmaßnahmen fast ausgeschlossen worden waren – letztendlich eine Bestätigung für gute Entwicklungsarbeit (Spalte 7 "A", Bild 3).

Entdeckungswahrscheinlichkeit "E" eines Fehlers

Die Kennzahl "E" bewertet die Wahrscheinlichkeit, mit der die Fehlerursache unter Berücksichtigung bereits geplanter Entdeckungsmaßnahmen erkannt wird. Entdeckungsmaßnahmen entdecken Fehlerursachen, die trotz aller Vermeidungsmaßnahmen auftreten. Spalte 4 in Tabelle 2 zeigt das Bewertungsschema. Eine 1 wird gesetzt, wenn der Fehler ziemlich sicher bei der Produktion oder in anschließenden Tests entdeckt wird. Eine 10 wird gewählt, wenn der Fehler nicht erkannt wird, da die Funktion oder das Merkmal nicht geprüft wird oder nicht geprüft werden kann.

Die Fehlerursache "falsche LED-Helligkeitsgruppe gewählt" (Nr. 2 in Bild 3) wird beim 100%-Ausgangstest des LED-Einsatzes sicher erkannt. Wir bewerteten die Entdeckungswahrscheinlichkeit somit mit 1. Die Fehlerursache "Wellenlänge verschiebt sich durch Strom und Temperatur" (Nr. 3 in Bild 3) bleibt dagegen unentdeckt und erhielt deshalb eine 10: Die Wellenlänge des LED-Einsatzes wird beim Ausgangstest nicht gemessen und die feinen Abweichungen sind mit bloßem Auge nicht erkennbar.

Die Risikoprioritätszahl (RPZ)

Anschließend errechneten wir für jede Fehlerursache die Risikoprioritätszahl (Spalte 10 "RPZ" in Bild 3). Sie gibt eine Rangfolge der Risiken innerhalb eines Systems an. Allerdings gibt sie kein absolutes Risiko an, da Risikoprioritätszahlen verschiedener FMEA-Projekte nicht verglichen werden können. Die Einzelbewertungen B, A und E werden innerhalb eines FMEA-Teams immer subjektiv gefällt. Weiterhin ist offensichtlich, dass die RPZ zwar ein

erhöhtes Risiko anzeigt, aber darüber hinaus nur eine geringe Aussagekraft besitzt. So kann eine RPZ von 100 durch verschiedene Szenarien entstehen: z.B. $A = 10$, $B = 10$ und $E = 1$ oder $A = 5$, $B = 5$ und $E = 4$ usw.



Achten Sie bei der Risikobeurteilung neben der RPZ immer auf hohe Einzelbewertungen!

Schritt 5: Interpretation und Risiko-Optimierung des Produkts

Die FMEA-Tabelle (Bild 3) wird nach hohen RPZ-Werten und hohen Einzelbewertungen abgesucht. Für diese werden mögliche Verbesserungsmaßnahmen diskutiert. Ein definiertes Team arbeitet die vielversprechendsten Ansatzpunkte aus und stellt zum vereinbarten Termin die Ergebnisse vor. Eine geeignete Maßnahme wird ausgewählt und zusammen mit Verantwortlichem und Zeitrahmen zur Umsetzung in das Formblatt eingetragen. Wird das Konzept geändert, muss anschließend die FMEA neu durchlaufen werden.

Es gilt folgende Rangfolge bei den Optimierungsmaßnahmen:

9. Konzeptänderung, die die Fehlerursache ausschließt bzw. deren Bedeutung erniedrigt (d.h. Kennzahlen A und / oder B verkleinern)
10. Erhöhung der Konzeptzuverlässigkeit, um die Auftretenswahrscheinlichkeit der Fehlerursache zu minimieren (d.h. Kennzahl A verringern)
11. Wirksamere Entdeckung der Fehlerursache (d.h. Kennzahl E reduzieren). Dies sollte nach Möglichkeit durch Verbesserungen in der Konstruktion geschehen, da zusätzliche Messungen in der Produktion Zeit und Geld kosten.

Anhand von drei Beispielen aus dem vorgestellten Entwicklungsprojekt illustriere ich im Folgenden, wie dies in der Praxis konkret aussehen kann.

Ein Sensor für die Helligkeit muss her!

Der höchste Wert der RPZ von 400 (Fehler Nr. 2 in Bild 3) ergab sich für den Fehler, dass die LEDs vorzeitig altern und damit vor dem regulär geplanten Austausch die Helligkeit unterhalb des Normwertes sinkt. Die in der Ansteuerung implementierte Fehlerabschaltung erkennt dies nur, wenn sich gleichzeitig die elektrischen Eigenschaften der LEDs ändern. Langzeittests an LEDs hatten aber gezeigt, dass dies oft nicht der Fall ist ($A = 4$), d.h. der LED-Einsatz leuchtet zu schwach und stellt ein Sicherheitsrisiko dar (Bedeutung 10). Dieser Fehler wird nicht automatisch entdeckt ($E = 10$). Die FMEA machte deutlich, dass hier akuter Handlungsbedarf bestand.

Eine strategische Entscheidung wird erforderlich

Im Grunde hatten wir das geahnt, aber die FMEA führt uns dieses Risiko direkt vor Augen und dokumentierte den dringenden Handlungsbedarf. Das Entwicklungsteam erhielt daraufhin die Aufgabe, Lösungen zu erarbeiten und

mit Schätzung der Zusatzkosten und Zeitverzögerung dem Management in zwei Wochen vorzustellen. Das Entwicklungsteam schlug als beste und einzige Lösung eine Überwachung des LED-Lichts im Einsatz durch einen optischen Sensor vor. Der Zielpreis konnte trotz der Zusatzkosten gehalten werden. Allerdings ließ die prognostizierte Dauer von sechs Monaten für die Implementierung den Zeitpunkt für die Produkteinführung platzen.

Unter diesen Umständen war eine Entscheidung des Managements erforderlich. Das Management beschloss, zweigleisig zu fahren: Die Produktentwicklung wurde einerseits – wie ursprünglich geplant – ohne Sensor fortgeführt, um den Liefertermin einzuhalten. Parallel dazu wurde andererseits das Sensorkonzept entwickelt, so dass in absehbarer Zeit ein LED-Einsatz mit Sensor zur Verfügung stand.

Zwei Maßnahmen retten das Produkt

Hintergrund war, dass unsere Kunden vor großflächiger Installation neuer LED-Einsätze längere Feldtests durchführen, um die Kompatibilität zwischen der Elektronik des LED-Einsatzes und dem Steuergerät zu prüfen. Die elektronische Schnittstelle zum Steuergerät wird durch den optischen Sensor nicht geändert, so dass die Ergebnisse dieser Tests auch für die Variante mit Sensor Gültigkeit hatten. Um das Risiko der Degradation zu reduzieren, wurden **LEDs mit höheren Helligkeitsgruppen** verbaut. Das grundsätzliche Problem wurde damit zwar nicht gelöst, aber der Zeitpunkt verschob sich, ab dem der Lichtstrom den Grenzwert 200 lm unterschreiten könnte. Durch diese erste Maßnahme sank die Auftretenswahrscheinlichkeit auf 2, die RPZ damit auf 200.

Die **zusätzliche Implementierung des optischen Sensors** verringerte nach einer ersten Abschätzung die Bedeutung der Fehlerfolge auf 4 (analog zur bereits implementierten Abschaltung bei falscher Stromaufnahme). Damit lag die RPZ bei einem akzeptablen Wert von 80. Diese Maßnahme verringerte zugleich die Bedeutung der Fehlerfolge "LED-Degradation aufgrund zu hoher Betriebstemperatur" (Nr. 5 in Bild 3) von 10 auf 4, da der optische Sensor auch bei dieser Fehlfunktion den LED-Einsatz definiert abschaltet.

Diese Abschätzung musste natürlich, sobald das Sensorkonzept vorlag, nochmals überprüft und verifiziert werden.

Konzeptverfeinerung schließt Fehlerursache aus

Die Fehlerursache "Wellenlänge verschiebt sich durch Strom und Temperatur" wird zum einen nicht entdeckt und hat eine mittlere Auftretenswahrscheinlichkeit ($A = 4$). Die Fehlerfolge wurde aufgrund möglicher Regressforderungen bei Nachmessen der Signale relativ hoch bewertet ($B = 9$). Die empfohlene Maßnahme lautete: "Die Abweichung der LED-Wellenlänge von dem im Datenblatt angegebenen Wert beim gewählten Strom und der maximal spezifizierten Temperatur von 80°C am T_c -Punkt wird anhand von Messungen ermittelt. Die LEDs, bei denen durch diese Abweichung die Wellenlänge des LED-Einsatzes außerhalb des erlaubten Bereichs liegen würde, werden nicht verwendet. Die Produktdokumentation wird entsprechend geändert."

Dieser Schritt verringert die Auftrittswahrscheinlichkeit von 4 auf 1, die RPZ liegt dann bei 90.

Nicht alle Fehler müssen behoben werden!

Es gibt keine klare Regel, ab welcher Höhe der RPZ oder von Einzelbewertungen Optimierungsmaßnahmen getroffen werden müssen. Es liegt in der Verantwortung des FMEA-Teams, solche Entscheidungen gemeinsam unter Betrachtung der jeweiligen Fehlfunktion zu diskutieren und zu treffen. So akzeptierten wir die RPZ von 120 mit einem E von 10 (Nr. 1 in Bild 3), da der implementierte Abschaltmechanismus für den Kunden und uns Sicherheit garantiert, obwohl der Austausch des LED-Einsatzes zusätzlicher Aufwand darstellt.

FMEA – für Produktsicherheit so wichtig wie die Spezifikation

Eine FMEA-Tabelle ist immer ein lebendiges Dokument: Nach Ausarbeitung der Konzeptänderung wird die FMEA-Tabelle aktualisiert. Die Qualitätsabteilung stellte unser Dokument über das interne Dokumentenmanagementsystem für zukünftige Projekte zur Verfügung. Die FMEA begleitet somit ein sicherheitskritisches Produkt über seinen gesamten Lebenszyklus hinweg.

Wir führten für unser LED-Board erstmalig eine Design-FMEA durch und sind davon überzeugt, dass diese Entscheidung wichtig für den Produkterfolg war. Zwei abgeleitete Maßnahmen verbesserten das Produktkonzept und erhöhten die Betriebssicherheit. Dies hat dazu beigetragen, dass Ampeln mit LED-Technik mittlerweile aus dem Straßenverkehr nicht mehr wegzudenken sind.

Literatur

- Pfeuffer, Hans-Joachim: FMEA – Fehler-Möglichkeiten- und Einfluss-Analyse, Hanser Verlag München, 2015
- Verband der Deutschen Automobilindustrie (VDA) (Hrsg.): Qualitätsmanagement in der Automobilindustrie. Sicherung der Qualität in der Prozesslandschaft, Band 4: Produkt- und Prozess-FMEA, 2. überarbeitete Aufl. 2006

Herausforderung und Verantwortung für jeden einzelnen

Informationssicherheit und Projekte



Klaus Schopka
Geschäftsführer der
Projektmanagement
Schopka GmbH

Management Summary

- Der Umgang mit Informationen und Informationstechnologie ist im Alltag jedes Projektleiters allgegenwärtig und untrennbar mit IT-Sicherheit und deren Grundwerten "Vertraulichkeit", "Integrität" und "Verfügbarkeit" verbunden.
- Wie sehr die Projektarbeit von Bedrohungen der Informationssicherheit durchzogen ist, zeigen typische Alltagssituationen.
- In den verschiedenen Projektphasen wird die IT-Sicherheit umfassend beeinflusst, oft ohne dass es uns bewusst ist.
- Da IT-Sicherheit Ressourcen, Zeit und Geld bindet, sind Konflikte vorprogrammiert. Das Thema muss daher bereits in der Planungsphase sorgfältig berücksichtigt werden.
- IT-Sicherheit liegt im Eigeninteresse von Projekten. Fehlende IT-Sicherheit wirkt sich negativ auf das Projekt und die Projektergebnisse aus.
- Sieht man IT-Sicherheit nur als technisches Thema, greift das zu kurz. IT-Sicherheit kann nicht delegiert werden, sie funktioniert nur, wenn alle Projektbeteiligten zusammenarbeiten und Verantwortung übernehmen.

"Projekte und Informationssicherheit?" Automatisch denkt man dabei an IT-Projekte, bei denen IT-Sicherheit, als Teil der Informationssicherheit, immer eine wichtige Rolle spielt. Betrachtet man jedoch die verschiedenen Dimensionen der IT-Sicherheit – Vertraulichkeit, Integrität und Verfügbarkeit von Daten, Dokumenten und Systemen –, wird schnell deutlich, dass das zu kurz gedacht ist. IT und deren Verwendung durchdringt zunehmend die Arbeits- und Projektwelt. Ohne IT-Einsatz sind z.B. Kommunikation und Dokumentation in Projekten kaum mehr vorstellbar. Auch der Einsatz von Projektmanagement-Software ist bei komplexen Projekten oder in Multiprojektumgebungen nicht mehr wegzudenken.

Dieser Beitrag verdeutlicht anhand von Beispielen aus dem Projektalltag, wie weitreichend die Bedeutung von Informationstechnologie und IT-Sicherheit ist und sensibilisiert dafür, dass alle an Projekten Beteiligten Verantwortung übernehmen müssen.

Exkurs: Jeder trägt die (Mit-)Verantwortung für Sicherheit!



Die gut erhaltene mittelalterliche Altstadt von Regensburg ist ein bekanntes Weltkulturerbe der UNESCO. "Stadtluft macht frei!" hieß es damals. Eine Grundvoraussetzung für diese Freiheit waren Schutz und Sicherheit, die Städte damals boten. Dies wurde durch Gräben, Mauern, Türme und Tore erreicht, wie das Modell im Stadtmuseum von Regensburg deutlich zeigt.

Wichtiger noch als die sichtbaren Bauwerke, war die Zusammenarbeit der Bürger. Berufswächter gab es nur wenige. Die waren viel zu teuer! Die Hauptlast trugen die Bürger und damit auch direkte (Mit)Verantwortung für die Sicherheit der Stadt! Sicherheit wurde schon damals großgeschrieben.

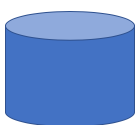
Was versteht man unter IT-Sicherheit eigentlich genau?

IT-Sicherheit oder IT-Security sind abstrakte Begriffe, deren Bedeutung für Laien schwer zugänglich ist. Eine leichter erfassbare Beschreibung liefert das Bundesamt für Sicherheit in der Informationstechnik (BSI): "IT-Sicherheit beschäftigt sich an erster Stelle mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung." Bezieht man auch die Informationen mit ein, die z.B. auf dem Papier oder in den Köpfen der Menschen gespeichert sind, lautet der hierzu passende Begriff "Informationssicherheit".

Der vorliegende Artikel verwendet bewusst meist den Begriff "IT-Sicherheit". Das bedeutet keinesfalls, dass die Sicherheit gedruckter Informationen oder verbale Kommunikation zu vernachlässigen sei. Vielmehr trägt es der Tatsache Rechnung, dass elektronisch gespeicherte und verarbeitete Daten und Informationen zunehmend Bedrohungen ausgesetzt sind.

Die Objekte der Sicherheit

Daten und Informationen



Nutzen erzeugen

Daten verarbeiten:

Software (Betriebssysteme, Anwendungen, „Apps“)

Netzwerk (LAN, WAN, WLAN)

Hardware (PC, Server, Smartphones, Rechenzentren)

Daten und Informationen sind wertvoll, denn sie sind der Rohstoff und das Kapital der modernen Wirtschaft und Gesellschaft. Diesen Wert hätten sie nicht, wenn sie nicht genutzt werden könnten. Dazu ist die Verarbeitung mit Hilfe von Software, Netzwerken und Hardware notwendig.

Die Objekte der Sicherheit sind somit festgelegt: Es sind zum einen die Daten und Informationen, zum anderen die zur Datenverarbeitung eingesetzte Hard- und Software sowie die benötigten Netzwerke (Bild 1).

Bild 1: Bausteine der Informationstechnologie

Was bedeutet "Sicherheit" genau?

Als nächstes müssen wir den Begriff der Sicherheit näher beschreiben. Dafür bieten sich die klassischen Dimensionen der IT-Sicherheit an, die auch für den erweiterten Begriff der Informationssicherheit gültig sind:

- **Vertraulichkeit** (Confidentiality): Vertrauliche Informationen müssen wir vor unbefugter Preisgabe schützen.
- **Integrität** (Integrity): Die Daten sind vollständig und unverändert.
- **Verfügbarkeit** (Availability): Dem Benutzer stehen Dienstleistungen, Funktionen eines IT-Systems oder auch Informationen zum geforderten Zeitpunkt zur Verfügung.

Mit dieser einfachen Übersetzung des Begriffes "Sicherheit" in Themen, die bearbeitet und umgesetzt werden können, sind auch die Handlungsfelder der IT-Sicherheit greifbar.

IT-Sicherheit und Projekte

Ein Projekt ist "ein einmaliges, zeitlich befristetes, interdisziplinäres, organisiertes Vorhaben, um festgelegte Arbeitsergebnisse im Rahmen vorab definierter Anforderungen und Rahmenbedingungen zu erzielen" (GPM, Individual Competence Baseline für Projektmanagement, 2/2017, S.29). Diese Definition lässt bereits erkennen, welche zentrale Bedeutung Kommunikation und Dokumentation für den Erfolg eines Projektes haben.

Merkmale von Projekten	Merkmale IT-Sicherheit
<ul style="list-style-type: none"> • zeitlich begrenzt • temporäre Teams • ergebnisorientiert – Änderungen 	<ul style="list-style-type: none"> • zeitlich unbegrenzt • Linienfunktion • ergebnisorientiert – Stabilität
<ul style="list-style-type: none"> • begrenzte Ressourcen 	<ul style="list-style-type: none"> • begrenzte Ressourcen
<ul style="list-style-type: none"> • werden von Menschen gemacht 	<ul style="list-style-type: none"> • wird von Menschen gemacht

Bild 2: Vergleicht man die Merkmale von Projekten und IT-Sicherheit, fallen zwei Konfliktfelder auf: Die zeitliche Dimension und die Konkurrenz um Ressourcen. Auf welche Weise mögliche Konflikte gelöst werden, hängt u.a. vom Menschen bzw. der Unternehmenskultur ab.

Vergleichen wir die Merkmale von Projekten mit denen der IT-Sicherheit, fallen sofort zwei Konfliktfelder ins Auge (Bild 2):

1. IT-Sicherheit ist auf Dauer und Stabilität ausgelegt. Projekte sind im Gegensatz dazu zeitlich begrenzt; die Projektteams lösen sich nach Fertigstellung wieder auf.
2. Beide Themen konkurrieren um begrenzte Ressourcen.

Wer setzt sich im Konfliktfall durch? In beiden Fällen entscheiden darüber u.a. die gelebte Kultur und die Werte im Unternehmen.

Aus dem Leben eines Projektleiters – Informationssicherheit im Alltag

Anhand einiger typischer Alltagssituationen möchte ich für das Thema Informationssicherheit

sensibilisieren. Die folgenden Beispiele reichen von der Fahrt mit der S-Bahn in die Arbeit bis zum Projektstatusmeeting per Konferenzsystem. In Bezug auf die Informationssicherheit zeigen die Beispiele Folgendes:

- Egal, was in Projekten geschieht, das Thema Informationssicherheit ist nie weit.
- Die Informationssicherheit ist in Projekten laufend gefährdet, oft durch Kleinigkeiten, die uns nicht weiter auffallen.
- Jeder(!) im Projekt beeinflusst die Informationssicherheit.

- Es geht primär nicht um Technik, sondern vor allem um das korrekte Handeln von Menschen.

Fahrt in die Arbeit

Für Kundentermine in München nutze ich regelmäßig die S-Bahnlinie 8, die Flughafenlinie. Besonders am Morgen und am Nachmittag fallen die einheitlich nach vorne geneigten Köpfe der Fahrgäste auf. Einige wenige sind einfach noch – oder schon wieder – müde oder lesen Zeitung. Die Mehrzahl aber blickt gebannt auf Smartphones, Tablets oder Notebooks, vereinzelt auch auf Papierdokumente oder Bücher. Kaum jemand realisiert, wie einfach ich vieles mitlesen kann.

Privat mag das in Ordnung sein. Handelt es sich aber um Emails, Präsentationen oder Schriftstücke aus dem beruflichen Umfeld, sieht das anders aus. Sehr schnell wandert hier die eine oder andere Information zu Personen oder an Stellen, wo sie nichts verloren hat. Vertraulichkeit wird hier klein geschrieben. Dabei gibt es oft wirklich einfache Lösungen, wie Blickschutzfolien oder einfach darauf zu achten, dass niemand mitlesen kann.

Am Flughafen

Die Situation ist ähnlich am Flughafen, der Endstation meiner S-Bahn. Was hier in kleinem Kreis oder in Gruppen besprochen wird, ist manchmal schon mehr als fahrlässig und kann im Einzelfall als Verstoß gegen Vertraulichkeits- und Geheimhaltungsvereinbarungen gelten. Die Ergebnisse der letzten Kundentermine muss man nicht in aller Öffentlichkeit verbreiten und dabei vielleicht noch Kommentare zu den Kunden und deren Mitarbeiter abgeben. Fazit: Vertraulichkeit – Fehlanzeige! Einzelfall – Fehlanzeige!

Eine kleine Zusatzinformation zum Umgang mit IT-Geräten in Zügen oder an Flughäfen: Eine kleine Studie aus 2016 hat ermittelt, dass an den sieben größten Flughäfen in Europa ca. 600 bis 700 Notebooks gefunden werden – pro Woche! Womöglich mit den Unterlagen zu einem Forschungsprojekt, einer Akquisition oder ähnlichem? Wenn dann nicht zumindest die Festplatte verschlüsselt ist ... Doch selbst solche Sicherheitsmaßnahmen lassen sich heute mittlerweile umgehen.

Fahrt im Zug

Ein Erlebnis bei einer Zugfahrt hat mir zu denken gegeben. Eine Sitzreihe hinter mir im ICE saß offenbar ein Vertriebsmitarbeiter einer Softwarefirma. Er hat einen Entwickler des Unternehmens angerufen um festzustellen, ob dieser einige zusätzliche Aufgaben für den Kunden übernehmen kann. Das Ganze unter Nennung des Kunden und der Ansprechpartner, Aufgabeninhalte und vertragsrelevanter Details. Ein Konkurrent hätte jetzt ein leichtes Spiel gehabt, speziell als sich herausstellte, dass die Softwarefirma nur Teile der gewünschten Aufgaben zeitlich unterbringen konnte. Fazit: Vertraulichkeit – Fehlanzeige! Einzelfall – Fehlanzeige!

Termin mit dem Auftraggeber

Der kaufmännische Leiter als Projektauftraggeber hat zur Abstimmung einiger "offener Punkte" kurzfristig um Rücksprache gebeten. Bei dem Projekt – das nachfolgend als Beispiel dienen soll – geht es darum, einige Backoffice-Funktionen des Unternehmens – eines europaweit agierenden Finanzdienstleisters – in einem Shared Service Center zusammenzufassen. Was genau "offen" ist, hat er nicht erwähnt.

Im Termin erklärt der kaufmännische Leiter, dass jetzt zusätzlich auch die Tochtergesellschaften in Österreich und der Schweiz in das Projekt mit einbezogen werden sollen. Zudem wird eine Reihe zusätzlicher Funktionalitäten benötigt. Der Projektleiter weist darauf hin, dass dies mit erheblichen, zusätzlichen Kosten verbunden ist und den Projektabschluss verzögern wird. Beides lässt der Auftraggeber nicht gelten. Schließlich habe der Projektleiter ja sicherlich genügend Puffer und Ressourcen eingeplant.

Der Termin endet mit dem Auftrag an den Projektleiter, einen Realisierungsvorschlag für alle Funktionalitäten zu erstellen – ohne Terminverschiebung. Etwas höhere Kosten akzeptiert der Auftraggeber. Welche Optionen hat der Projektleiter? Was schlagen Sie vor?

Vorhandene Terminpuffer kann er nicht einsetzen, da die Planung ohnehin schon optimistisch erstellt werden musste. Neudeutsch: Best case! Zusätzliche Ressourcen einzusetzen, erhöht die Kosten und führt erfahrungsgemäß zu Verzögerungen (Brooks'sches Gesetz). Bleibt also der Bereich der Leistungen. Funktionalitäten der Anwendung dürfen laut Vorgabe nicht ernsthaft eingeschränkt werden.

Was bleibt noch an Einsparpotential? "Sonstige Aufgaben" im Projekt, wie Aufgabenvorbereitung, Planung, Test, Retest, Integration, Dokumentation und Schulung. Was dabei auch mit auf der Strecke bleibt, sind die darin enthaltenen Aufgaben und Ressourcen für die IT-Sicherheit. Dem Projektleiter bleibt lediglich die Option, diese Schwachstellen zu dokumentieren und sie gegenüber dem Auftraggeber aktiv zu vertreten.

Statusmeeting

Der nächste Höhepunkt des Tages ist das regelmäßige Projektstatusmeeting. Da kann der Projektleiter ja auch gleich die neue Situation vorstellen! Für das Meeting ist ein Besprechungsraum gebucht. Die Mitarbeiter der Dienstleister wählen sich aus ihren Firmen oder dem Homeoffice in das Konferenzsystem ein. Die notwendigen Unterlagen werden vorab an die Teilnehmer per Email verschickt.

Die Besprechung verläuft, wie zu erwarten war. Die neuen Aufgaben sind alle machbar – aber nicht in der vorgegebenen Zeit. Das Facility Management muss zusätzliche Büroflächen am neuen Standort schaffen, der Personalbereich sieht einen Berg neuer Vertragsänderungen vor sich und rätselt ob der Betriebsrat schon informiert ist. Der Vertreter der IT fragt, wer denn die zusätzlichen Arbeiten leisten soll. Lösung gibt es natürlich noch keine. Die Teilprojekte werden die Anforderungen bis zum nächsten Meeting prüfen und bewerten. Das Projektteam beschließt ab sofort, den Status sowie Ergebnisse und Probleme permanent auszutauschen. Die Möglichkeit dazu bietet ein bereits im Projekt verwendetes, externes Projektmanagement-Portal, das jetzt intensiv auch grenzübergreifend durch Teilprojekte, Entwickler und IT-Spezialisten genutzt werden soll.

Soweit klingt das alles ganz normal. Aus dem Blickwinkel der IT-Sicherheit jedoch wirft die kurze Beschreibung des Meetings bereits eine Reihe von Fragen auf: Welche internen und externen Personen nehmen am Meeting teil? Wer kontrolliert? Wie ist der Zugriff auf das Projektmanagementportal geregelt? Wer erteilt Zugriff? Gibt es Rollen, mit denen vertrauliche Informationen geschützt werden? Wie wird verhindert, dass vertrauliche Informationen, wie z.B. Firewall Regeln, Mitarbeiterlisten, Netzwerkadressen usw. geschützt bleiben? Gibt es eine Versionierung von Unterlagen und Informationen, mit der auseinanderdriftende Wissensstände verhindert werden, sodass die Projektbeteiligten nicht aneinander vorbei arbeiten?

Die genannten Beispiele sind nur einige kurze Episoden aus einem Projekt. Die Liste lässt sich beliebig erweitern.

Einfluss auf die IT-Sicherheit in den Projektphasen

Fazit der oben genannten Beispiele ist, dass speziell die Themen "Vertraulichkeit" und "Verfügbarkeit" des Projektergebnisses einer Vielzahl von Schwachstellen ausgesetzt sind. Als Gedankenanstoß zeigt Bild 2 exemplarisch für das Beispielprojekt, wie die Grundwerte der IT-Sicherheit im Projektablauf beeinflusst werden. Ich bin überzeugt, Sie können die Beispiele fortführen. Die Sammlung ist aber ausreichend, um das weite Themenfeld anzudeuten und erste Hinweise zu einfachen Lösungen aufzuzeigen.

Zur leichteren Orientierung nehme ich im Text Bezug auf die Nummerierung der einzelnen Kästchen in Bild 2 ([1] bis [15]).

	Dimensionen der Informationssicherheit und IT-Sicherheit		
	Vertraulichkeit	Verfügbarkeit	Integrität
Ideen- / Start-Phase	Vertrauliche Informationen an Berater; Vertrauliche Informationen an Lieferanten; Unkontrollierte Kommunikation; Sensible Geschäfts- und Planungsdaten in Business Case	Schnell etwas ausprobieren; Ressourcen unkoordiniert für schnelle Tests oder Konzepte einbinden; Motivation der Anwender; Qualifikation der Anwender	Testfälle, Testdaten einspielen; Veraltete Dokumentationen verwenden
Planungs-Phase	Keine Verwaltung der Zugriffsrechte; Nicht abgesicherte Pilotinstallationen; Kein Sicherheitskonzept für Projektunterlagen; Integrität der Projektmitarbeiter	Keine Validierung von Annahmen zur Ist-Situation; Ausfallsicherheit unzureichend geplant; Notfallkonzept fehlt; Unzureichende Konfigurationsplanung; Datensicherungskonzept; Nutzer zu wenig einbezogen	Unzureichendes Rechtekonzept in der Anwendung; Unzureichende Testfälle; Kein Datensicherheitskonzept
Umsetzungs-Phase	Zugang Produktivsysteme; Testdaten nicht anonym; Trennung Test und Produktion; Keine Verwaltung der Zugriffsrechte; Datenschutz grenzüberschreitend	Trennung Test und Produktion; Last- und Performance zu wenig getestet; Vorzeitige Kündigung von Altverträgen; Neue Anforderungen werden "schnell" eingebaut	Zugriff Produktionsdaten; Trennung Test und Produktion; Unzureichende Tests; Neue Anforderungen werden nicht ausreichend integriert
Abschluss-Phase	Keine Bereinigung der Zugriffsrechte; Sensible Sicherheitsdaten nicht ausreichend geschützt	Performance für Anwender; Ergonomie der Anwendung; Unzureichende Schulungen für Nutzer; Offene Punkte und Funktionalitäten; Notwendige Nacharbeiten	Keine Bereinigung Zugriffsrechte; Keine einheitliche Dokumentation; Unzuverlässige Schnittstellen; Datensicherungskonzept unzuverlässig
Nutzungs-Phase	Zugriffsrechte von Fachbereichen und Externen; Nicht abgesicherte Internetseiten; Datenhaltung in unsicheren Netzen	Datenhaltung in unsicheren Netzen; Performance für Anwender; Ergonomie der Anwendung; Kein Test Notfalllösung; Datensicherungskonzept	Zugriffsrechte von Fachbereichen und Externen; Datenhaltung in unsicheren Netzen

Tabelle 1: Die Einflussnahme auf IT-Sicherheit im Beispielprojekt

Ideenphase

Die Beispiele aus S-Bahn, Flughafen oder Zug betreffen bereits die Ideenphase (Tabelle 2, 1-3), in der vertrauliche Informationen mit Beratern und Lieferanten ausgetauscht werden oder in den Business Case einfließen.

Vertrauliche Informationen müssen als solche erkennbar sein und sorgfältig behandelt werden. Ideen, die als wichtig erachtet werden, sollten schnell in ein Projekt oder eine Vorstudie gefasst werden, um einen Ordnungsrahmen herzustellen. Bereits bei den ersten Abstimmungsrunden kann das initiale Projektteam grob ermitteln, inwieweit sicherheitsrelevante Themen berührt sind (initiale Schutzbedarfsanalyse und Risikoanalyse) und geeignete Regeln zum Umgang damit festlegen.

Kommunikation sollte nur über die dafür festgelegten Kanäle erfolgen. Für den Umgang mit vertraulichen Informationen muss für alle Teammitglieder eine hinreichende Vertraulichkeitsverpflichtung vorliegen, sei es projektbezogen oder im Rahmen von Arbeitsverträgen. Vorher dürfen keine konkreten Informationen oder Dokumente weitergegeben werden. Sie meinen, das ist selbstverständlich? Oft ja, aber fragen Sie als Projektleiter im Zweifelsfall lieber nach – nicht nur für externe Mitarbeiter.

Auch die Grundwerte der Verfügbarkeit und Integrität können in der Ideenphase betroffen sein. Im Beispielprojekt besteht z.B. die Gefahr, schnell etwas ausprobieren oder einige "Testfälle" durchspielen zu wollen. Womit dann im schlimmsten Fall auch die Integrität von Datenbeständen gefährdet ist.

Planungsphase

Mit dem Einstieg in die Planungsphase (Tabelle 2, 4-6) nimmt das Volumen an Informationen rapide zu. Parallel wächst in der Regel auch das Projektteam. Fehlt in der Planungsphase z.B. ein Sicherheitskonzept für Projektunterlagen, gibt es keine Verwaltung der Zugriffsrechte, existieren nicht abgesicherte Pilotinstallationen oder ist die Integrität der Projektmitarbeiter nicht sichergestellt, gefährdet das die Vertraulichkeit von Informationen.

Frühzeitige Analyse des Schutzbedarfs zahlt sich aus

In dieser Phase wird festgelegt, was erledigt werden muss, um die gewünschten Projektergebnisse bereitzustellen. Dazu gehören auch alle Maßnahmen, die ein notwendiges Niveau an IT-Sicherheit für die Projektergebnisse und die Prozesse zu deren Erstellung gewährleisten. In der Planungsphase zahlt es sich daher aus, wenn der Schutzbedarf frühzeitig analysiert wurde.

Die Analyse des Schutzbedarfs führt zu zahlreichen Vorgaben auf der technischen Seite, z.B. welche sicherheitsrelevanten Lösungen verwendet werden müssen. Dazu zählen Themen wie Verfügbarkeit, Zugriffsschutz, Verschlüsselung oder Datensicherung. Konkret können aus der definierten Vertraulichkeitsstufe Vorgaben für die Ablage und Verteilung von Dokumenten, Zugriffsrechte von Projektmitarbeitern, Einsatz externer Dienstleister, Verhalten im öffentlichen Raum abgeleitet werden.

In einigen Unternehmen ist es z.B. gelebte Praxis, dass sensible Unterlagen nicht im öffentlichen Raum gelesen, bearbeitet oder besprochen werden dürfen. Diese Vorgaben zu kommunizieren, einzuführen und dauerhaft durchzusetzen ist klar die Aufgabe des Projektleiters in Zusammenarbeit mit dem Auftraggeber, Mitarbeitern aus den Sicherheitsbereichen und bei strengen Vorgaben auch mit der Unternehmensleitung.

Um die IT-Sicherheit zu gewährleisten, muss es in jedem Projekt eine feste Aufgabe sein, den Schutzbedarf schon bei Projektbeginn festzustellen, z.B. im Rahmen der Risikoanalyse. Der Aufwand für dieses Vorgehen ist mit etwas Vorbereitung gering, z.B. wenn Vorlagen verwendet werden und ein erfahrener Mitarbeiter den Workshop moderiert. Der Nutzen ist erheblich, das Vorgehen kann so nach kurzer Einübungsphase schnell zur gelebten Selbstverständlichkeit werden.

Umsetzungsphase

"Zielorientiertes Vorgehen" sollte keine festgelegten Regeln aushebeln

Eine besondere Herausforderung in der Umsetzungsphase (Tabelle 2, 7-9) ist die dauerhafte Einhaltung der zuvor festgelegten Regeln. Wer kennt nicht die Verlockung oder Forderung etwas

"hemdsärmeliger" oder "zielorientierter" vorzugehen, wenn Einführungstermine gefährdet sind, qualifizierte Ressourcen nur begrenzt zur Verfügung stehen oder hoher Zusatzaufwand zu erwarten ist. Dies gilt speziell, wenn der Auftraggeber Druck aufbaut!

In einer solchen Situation ist es vorteilhaft, auf ein Dokument verweisen zu können, das weitestgehend auf Angaben und Vorgaben des Auftraggebers beruht. Besteht er dennoch auf einem Vorgehen, das nicht den Anforderungen entspricht, muss der Projektleiter den Sachverhalt zumindest in einem Protokoll festhalten, oder bei kritischen Vorgängen eine schriftliche Übernahme der Verantwortung verlangen. Das ist zwar keine perfekte Lösung, aber zumindest eine bewusste Entscheidung, die zu nochmaligem Überdenken anregt.

Saubere Trennung der Zugriffsrechte für den Datenschutz

Klassiker in Bezug auf die IT-Sicherheit ist die saubere Trennung von Entwicklung, Test und Betrieb, um Risiken für die produktive IT auszuschließen. Dies gilt nicht nur für die eigentlichen IT-Systeme, sondern vor allem auch für Daten, Berechtigungen und Dokumentationen. Das Thema Daten wird aktuell durch die neue DSGVO thematisiert. Weniger Beachtung findet immer wieder die Trennung der Zugriffsrechte. Entwickler, egal ob intern oder extern, sollten z.B. keinen direkten Zugriff auf produktive Systeme erhalten, auch wenn das im Einzelfall "praktisch" wäre.

Der Zugriff Projektbeteiligter auf sensible Informationen und Dokumentationen ist in vielen Fällen notwendig. IP-Adressen, Firewallregeln, detaillierte Netzpläne usw. sind allerdings nicht nur für das eigene Unternehmen interessant, sondern können auch für Cyber-Kriminelle von Nutzen sein. Auch Geschäftsunterlagen, Organisationspläne, Unternehmensplanungen und andere Dokumente, die im Rahmen eines Projektes genutzt werden, um z.B. einen Business Case zu erstellen oder Mengengerüste für IT-Planungen festzulegen, sollten nicht in falsche Hände gelangen. Die Verteilung solcher Informationen muss daher restriktiv gehandhabt werden. Das Haus verlassen sollten sie nie, da damit jede wirksame Kontrolle verloren geht.

Change-Management statt Hauruck-Aktionen

In der Umsetzungsphase entstehen oft neue Anforderungen durch den Auftraggeber oder es gibt Probleme in der Entwicklung oder bei der eigentlichen Umsetzung. Werden diese Anforderungen nicht durch ein etabliertes Change-Management kanalisiert, kommt es schnell zu Hauruck-Aktionen mit Auswirkungen auf alle Dimensionen der IT-Sicherheit. Die Aussage "Das haben wir gleich!" mag in der Entwicklung zulässig sein. Wenn betriebliche Systeme oder Daten betroffen sind, sollten Sie als Projektleiter jedoch einschreiten!

Abschlussphase

Die Abschlussphase (Tabelle 2, 10-12) regelt die Übergabe der Projektergebnisse an den Auftraggeber und die Beendigung des Projekts. Sie bietet die Gelegenheit zum großen Aufräumen. Dazu gehört z.B. alle Zutritts- und Zugriffsrechte zu bereinigen, Einträge im Active Directory anzupassen oder zu löschen und Projektverzeichnisse aufzuräumen und zu archivieren. Dokumentationen müssen in einer gültigen Version fertiggestellt, Anwender geschult, Altsysteme zurückgebaut werden und vieles mehr.

Diese Aufgaben kosten Zeit und sollten daher im Projektplan und Budget fest eingeplant sein. Wird hier "abgespeckt", wirkt sich das negativ auf die IT-Sicherheit aus.

Nutzungsphase

Nach Lehrbuch werden fertige Projekte bzw. Projektergebnisse an die Auftraggeber übergeben (Tabelle 2, 12-15). Wenn wir uns aber in Erinnerung rufen, wie das so in unseren letzten Projekten ablief, blieben vermutlich immer wieder Aufgaben unerledigt, Funktionalitäten wurden mit Workarounds ersetzt, Dokumentationen blieben Stückwerk, zusätzliche Anforderungen werden ad hoc umgesetzt und nicht getestet oder dokumentiert. Es gab Lücken, die nur teilweise dokumentiert und nicht immer mit dem Auftraggeber abgestimmt waren. Für deren Bereinigung wurde dann gerne auf Folge-Releases oder eben pauschal auf Nacharbeiten verwiesen.

Mangelnde IT-Sicherheit reduziert den Nutzen des Projektergebnisses

Solche unerledigten Aufgaben beeinflussen die IT-Sicherheit. Konsequenzen sind z.B. Datenhaltung in unsicheren Netzen, nicht abgesicherte Internetseiten, ungetestete Notfalllösungen, unzulängliches Datensicherungskonzept, zu geringe Performance für Anwender, schlechte Ergonomie der Lösung usw. Gibt es Einschränkungen bei der Verfügbarkeit, Vertraulichkeit oder Integrität, trifft das den Auftraggeber bei der Verwendung der Projektergebnisse und reduziert den erwarteten Nutzen oder stellt die Ergebnisse komplett in Frage. In unserem Beispiel konnten geplante Produktivitätsziele nicht erreicht werden, es entstanden Zusatzkosten wegen unzuverlässiger Schnittstellen und vieles mehr.

Bei der Entwicklung und Einführung neuer Produkte wäre es z.B. kritisch, wenn der geplante Nutzen nicht erreicht werden könnte, weil der Wettbewerb wegen mangelnder IT-Sicherheit bereits frühzeitig informiert war. Auch bei Start-Ups ist Vertraulichkeit existenziell, um nicht den, oft geringen, Entwicklungsvorsprung zu verlieren.

IT-Sicherheit ist kein reines Technik-Thema!

Der primäre Fokus vieler Projekte liegt auf der Umsetzung der funktionalen Anforderungen. IT-Sicherheit befindet sich hier in einem Dilemma, denn sie wird nicht als unverzichtbares Qualitätsmerkmal dieser Ergebnisse angesehen. Zudem gilt sie für viele als vorrangig technisches Thema. Die Verantwortung dafür wird dann den für Technik zuständigen Bereichen zugeschoben.

Technik ist jedoch nur einer von mehreren Bausteinen für IT-Sicherheit. Auch Organisation und Prozesse gehören zum IT-Sicherheitskonzept eines Projekts. Technik wird als Teil davon erst wirksam, wenn alle Projektmitarbeiter ein auf das Gesamtkonzept ausgerichtetes Verhalten zeigen.

Positive Aspekte der IT-Sicherheit

IT-Sicherheit verursacht nicht nur Aufwand, sondern bietet auch Chancen. Die wohl größte Chance liegt darin zu verhindern, dass sich Fehler, Fehleinschätzungen, Informationsdefizite oder Fehlinformationen negativ auswirken. Was das konkret bedeuten kann, zeigen folgende Beispiele.

Beispiel: Anwendungs-Verfügbarkeit falsch eingeschätzt

Wird im Projektbeispiel die geforderte Verfügbarkeit für die Anwendungen am Anfang als zu niedrig eingestuft und während der laufenden Umsetzung nach oben korrigiert, sind die Konsequenzen weitreichend: Es wird eine neue Architektur für Anwendung, Daten und Infrastruktur benötigt, zusätzliche Tests sind erforderlich, es braucht eine neue oder zusätzliche Hardware und vieles mehr. Unterm Strich entstehen also hohe Zusatzkosten und die zeitliche Verzögerung ist erheblich. Was wird der Auftraggeber davon halten? Wie sieht der Business Case jetzt aus? Eine Schutzbedarfsanalyse hätte hier vorbeugen können.

Beispiel: Vertrauensverlust durch fehlende Vertraulichkeit

Im Rahmen der Softwareumstellung überlegt der Auftraggeber, hier der CFO, bestimmte Verwaltungsaufgaben an externe Dienstleister zu vergeben und einige Abteilungen an einem Standort zu konzentrieren. Der Projektauftrag lautet, passende technische Szenarien dafür zu prüfen. Da noch keine Aussagen zu Machbarkeit und Wirtschaftlichkeit möglich sind, sind auch die Fachabteilungen noch nicht informiert. Informationen über entsprechende Konzepte und Tests gelangen jedoch aus dem Projekt an Mitarbeiter der betroffenen Abteilungen. Die Reaktionen der Mitarbeiter? Verunsicherung und Widerstand. Auch der weitere Ablauf des Projektes ist deutlich erschwert, da das Vertrauen erst einmal verloren ist.

Der grundlegende Fehler liegt beim CFO, der in diesem Change Projekt seine Mitarbeiter nicht rechtzeitig informiert und mitgenommen hat. Der Fehler liegt aber auch im Projekt. Hätte dieses im Rahmen der Informationssicherheit stärker auf die notwendige Vertraulichkeit geachtet, wären Gedanken zu einem Thema nicht falsch kommuniziert und als Tatsachen dargestellt worden. Der so bedingte Vertrauensverlust wäre vermieden worden.

Beispiel: Frühzeitige Optimierung von Lösungen

Die frühzeitige Auseinandersetzung mit den Grundwerten der IT-Sicherheit räumt die Chance ein, im Projekt nicht nur Standardlösungen zu implementieren, sondern gemeinsam mit Fachleuten wirklich gute und auf die Projektergebnisse zugeschnittene Lösungen auszuwählen und zu entwickeln.

Um das Beispiel der Anwendungs-Verfügbarkeit weiterzuspinnen: Zur Projektlösung gehört nicht nur der zuverlässige Schwenk auf einen anderen Rechner im Clusterverbund. Es gehören dazu auch Themen wie Performance für den Anwender, Integrität von Daten, Monitoring und einiges mehr.

Um ein solches Lösungspaket zu schnüren, müssen sich die kompetenten Fachkräfte frühzeitig abstimmen. Diesen Prozess muss der Projektleiter über die Grenzen der benötigten Fachgruppen hinweg steuern und moderieren. Und das ist nur möglich, wenn das Thema IT-Sicherheit frühzeitig ausreichend Raum erhält.

Was können wir also tun?

Die Beispiele zeigen deutlich, dass der Gebrauch von Informationstechnologie – auch in Projekten – für uns mittlerweile alltäglich geworden ist. Egal, was geschieht, die IT-Sicherheit ist nie weit und jeder(!) im Projekt beeinflusst diese. Oft sind es Kleinigkeiten, die uns nicht weiter auffallen, die die IT-Sicherheit gefährden. Oft sind es auch Dauerbrenner, die sich immer wiederholen, wie z.B. ein nachlässiger Umgang mit Berechtigungen, keine oder ungenügende Tests oder das unachtsame Verteilen von Informationen und Dokumenten. Um IT-Sicherheit zu gewährleisten, geht es vor allem darum, dass sich Menschen korrekt verhalten und korrekt handeln.

Was können wir also als Konsequenz tun? Wir können ...

- ... alles so belassen wie es ist: Diese Alternative löst kein Problem und stellt absolut niemand zufrieden.
- ... nach strengeren Regeln und Gesetzen rufen: Eine "Straßenverkehrsordnung" für IT hätte vielleicht einige Vorteile, aber der Vergleich mit der echten Straßenverkehrsordnung führt zur Frage, ob sich dadurch wirklich viel ändert. Das Verhalten der IT-Nutzer bleibt eine Grauzone.
- ... mehr technische Lösungen verlangen: Technik ist notwendig und Regeln zu mehr Qualität der technischen Lösungen sind hilfreich. Letztlich aber ist Technik für sich auch nicht die Lösung.
- ... bessere Informationen und Ausbildung verlangen: Hier liegt ein wichtiger Ansatzpunkt. IT-Nutzer und IT-Mitarbeiter dürfen nicht allein gelassen werden, sondern müssen verständliche Informationen zu Sicherheitsthemen und deren Konsequenzen erhalten. Das Projektmanagement ist hier gefordert, die kritischen Themen der IT-Sicherheit in den methodischen Ansätzen aufzunehmen.
- ... selbst sorgfältiger und achtsamer mit Informationen und IT-Hilfsmitteln umgehen: Dies ist ein unverzichtbarer und eigentlich gar nicht so schwieriger Ansatzpunkt für jeden!
- ... uns speziell beim Projektstart angewöhnen, sowohl das geplante Projektergebnis als auch unsere Projektumgebung einer Sicherheits- und Risikoanalyse zu unterziehen. Daraus können wir konkrete Anforderungen und Regeln für das Projekt und alle beteiligten Mitarbeiter ableiten.

Fazit – IT-Sicherheit liegt im Eigeninteresse von Projekten

Informationstechnologie und der Umgang mit Informationen sind im Alltag jedes Projektleiters allgegenwärtig. Sie sind untrennbar mit den Grundwerten der IT-Sicherheit verbunden. Dies gilt für alle mir bekannten Projekte, nicht nur in der Informationstechnologie.

Immer einfacher zu bedienende Endgeräte und "Apps" sorgen dafür, die Komplexität und ständige Präsenz der IT immer stärker zu verbergen. Uns ist kaum noch bewusst, dass wir IT nutzen und was diese im Hintergrund mit unseren Daten und Informationen macht. Umso wichtiger ist es, dafür ein neues Bewusstsein zu schaffen. Dies gilt für den privaten Bereich, umso mehr aber noch für den beruflichen Bereich, wie z.B. in Projekten.

Projekte und Projektmanagement zielen immer auf Veränderungen ab. Es ist wichtig, dafür zu sorgen, dass sich diese Änderungen nicht negativ auf die IT-Sicherheit auswirken – zumal Projektleiter oft mit sensiblen und vertraulichen Informationen umgehen. Gleichzeitig bieten Projekte die Chance, die IT-Sicherheit zu verbessern – gerade wegen der durchgeführten Änderungen.

IT-Sicherheit bindet Ressourcen, Zeit und Geld. Also alles, was in Projekten knapp ist. Konflikte sind hier vorprogrammiert und müssen in Projekten bereits in der Planungsphase berücksichtigt werden. Den Beteiligten muss bewusst sein, dass der Verzicht auf IT-Sicherheit teure Konsequenzen haben kann!

IT-Sicherheit entsteht aus einer Vielzahl von Mosaiksteinen, die wir in unterschiedlichen Ausprägungen zu einem Gesamtkonzept zusammenführen müssen. Grundlage sind die Anforderungen oder Qualitätsmerkmale des geplanten Projektergebnisses.

IT-Sicherheit ist kein Konsumgut! Sie entsteht durch unser Handeln und Verhalten. Unsicherheit entsteht durch Unterlassen.

IT-Sicherheit liegt im Eigeninteresse von Projekten: Ohne sie ist die Nutzung der Projektergebnisse nicht oder nur eingeschränkt möglich. Hieraus ergibt sich eine besondere Verantwortung der Projektleiter und des Projektmanagements. IT-Sicherheit und Informationssicherheit im Projekt funktionieren aber nur, wenn alle Beteiligten zusammenarbeiten und Verantwortung übernehmen! Wie war das noch mit der Sicherheit von Städten im Mittelalter?

Pragmatisches Bestimmen der Kritikalität von Lieferanten und deren Bauteilen

Risikomanagement in der Supply Chain

Management Summary

- Neben kürzer werdenden Produktlebenszyklen steigen sowohl Kundenanforderungen als auch Variantenvielfalt und Produktkomplexität. Diese Umstände erfordern eng verknüpfte und effiziente Supply Chains.
- Optimierte Supply Chains bergen eine Vielzahl an Risiken, die in der heutigen volatilen Umwelt kaum mehr wirtschaftlich abzusichern sind.
- Zum Risikomanagement in der Supply Chain werden häufig kostenintensive Sicherheitsbeständen aufgebaut und breite Lieferantenportfolios mit hohem Koordinierungsaufwand unterhalten.
- Die Unternehmensberatung Kemény Boehme & Company hat eine Methode in vier Schritten zur umfassenden Identifikation, Bewertung und Darstellung bestehender Risiken in einer Risikomatrix erarbeitet.
- Bei der Anwendung der Methode beim Kunden werden Risiken im Sinne eines zielgerichteten Risikomanagements priorisiert und ein effizienter Ressourceneinsatz sichergestellt.



Jonathan Isele

Manager bei der Kemény
Boehme & Company GmbH



Max Weidmann

Consultant bei der Kemény
Boehme & Company GmbH

Industrieunternehmen stehen heutzutage vor vielen Herausforderungen: Die fortschreitende Globalisierung und der damit verbundene Kostendruck sowie die ausbreitende Digitalisierung von Produkten und Produktionsprozessen sind nur zwei Beispiele hierfür. Neben immer kürzer werdenden Produktlebenszyklen steigen sowohl Kundenanforderungen als auch Variantenvielfalt und Produktkomplexität. So müssen zahlreiche Produkte in immer kürzerer Zeit kostenoptimal entwickelt und auf den Markt gebracht werden. Dies erfordert Supply Chains, in denen die jeweiligen Unternehmen über Landesgrenzen hinweg eng miteinander verknüpft sind und effizient agieren.

Nach einer Studie von Bendul und Brüning kommt es innerhalb solcher Supply Chains regelmäßig zu mittleren oder schwerwiegenden Störungen. Unterbrechungen in Material- oder Informationsfluss können demnach die Produktivität oder den Umsatz senken – und zwar unabhängig von der Branche.

Für Unternehmen stellen Störungen in den Supply Chains hohe Risiken dar, denen häufig mit dem Aufbau von Sicherheitsbeständen oder dem Unterhalt eines möglichst breiten und nachhaltig stabilen Lieferantenportfolios entgegengewirkt wird. Die klassischen Maßnahmen des Risikomanagements in der Supply Chain führen dabei zu einem sehr hohen Kosten- und Koordinierungsaufwand.

Zum Erhalt ihrer Wettbewerbsfähigkeit müssen Unternehmen heute die begrenzten Ressourcen (finanzielle Mittel, Personal etc.) möglichst effizient und effektiv einsetzen. Dieser Optimierungsdruck steht den oben genannten Maßnahmen des Risikomanagements gegenüber. Die optimierten und schlanken Supply Chains (reduzierte Sicherheitsbestände, konsolidierte und kostenoptimierte Lieferantenstruktur etc.) bergen eine Vielzahl an Risiken, die in der heutigen volatilen Umwelt kaum mehr wirtschaftlich abzusichern sind.

Durch die enge Kopplung von Supply Chains nach dem Just-In-Sequence Prinzip können auch kleinste Vorfälle erhöhte Kosten, Qualitätsprobleme oder Versorgungsengpässe für die gesamte Wertschöpfungskette bedeuten. So führen Qualitätsmängel bei einem nachgelagerten Lieferanten (n-Tier) möglicherweise zu Qualitätsproblemen und Produktionsausfällen beim Original Equipment Manufacturer (OEM). Folgen davon sind qualitätsbedingte Rückrufaktionen und verzögerte Auslieferungen mit entsprechendem Image-Schaden und Regressforderungen an betroffene Lieferanten. Die Herausforderung des Risikomanagements besteht darin, Supply Chain Risiken für das Unternehmen möglichst umfangreich zu managen und zeitgleich kostenoptimiert zu agieren.

Ansteigende Qualitätskosten bei unzureichendem Risikomanagement

Genau diesem Spannungsfeld – maximale Risikoreduzierung bei beschränktem Ressourceneinsatz – sah sich ein Automotive-OEM und Kunde der Unternehmensberatung Kemény Boehme & Company (KBC) gegenüber: Ein deutlicher Anstieg an lieferanteninduzierten Qualitätskosten deckte Mängel im Supply Chain Risikomanagement auf. Vor dem Hintergrund beschränkter personeller und finanzieller Ressourcen sollte ein ganzheitlicher und systematischer Ansatz zum Risikomanagement erarbeitet werden. Im dafür beauftragten Projekt kamen die beiden KBC Berater Jonathan Isele und Max Weidmann beim Kunden an der Schnittstelle zwischen Einkauf und Qualitätsmanagement zum Einsatz.

Ziel des Projektes war die Entwicklung eines Ansatzes zur Identifizierung, Bewertung und Priorisierung von Risiken entlang der Supply Chain. Dieser sollte den effizienten und zielgerichteten Einsatz von Ressourcen ermöglichen. Die umfangreiche und vernetzte Supply Chain des Kunden, die über 500 Lieferanten im In- und Ausland sowie entsprechende Sublieferanten-Strukturen umfasste, erschwerte die Aufgabenstellung zusätzlich.

Die methodische Erarbeitung der KBC Risikomatrix in vier Schritten

KBC hat eine Methode entwickelt, die diesen Herausforderungen gerecht wird. Sie setzt sich aus vier aufeinander aufbauenden Schritten zusammen und ist auf verschiedenste Anwendungsfälle übertragbar. Die Herangehensweise wird im Folgenden Schritt für Schritt generisch sowie anhand des konkreten Fallbeispiels mit dem Automotive-OEM beschrieben. Das Ergebnis ist eine Risikomatrix, welche sowohl die Lieferanten- als auch die entsprechende Bauteilkritikalität abbildet.

Schritt 1: Identifikation Risikotreiber

Zunächst sind die relevanten Risikotreiber zu identifizieren. Hierfür werden Aspekte definiert, die die jeweiligen Eigenschaften der Risiken beschreiben. Im klassischen Risikomanagement werden die möglichen Szenarien häufig bezüglich ihrer Eintrittswahrscheinlichkeit und (finanziellen) Auswirkung betrachtet. In der Praxis ist jedoch meist eine umfassendere Risikobetrachtung notwendig.

Im Anwendungsfall war die reine Betrachtung des Ausfallrisikos eines Lieferanten ebenfalls nicht ausreichend. Im Falle des OEM stellten die Lieferanten erst in Kombination mit den jeweils gelieferten Bauteilen die zentralen Risikotreiber dar. So verkörperte ein „kritischer Lieferant“ erst dann ein nennenswertes Risiko für das Unternehmen, sofern seine Bauteile für das Endprodukt als entsprechend kritisch eingestuft wurden. Die Risikotreiber waren wiederum von noch zu definierenden Einflussfaktoren abhängig. Bild 1 zeigt eine schematische Darstellung zur Identifikation von Risikotreibern und deren Einflussfaktoren.



Bild 1: Schematische Darstellung Schritt 1 (Identifikation Risikotreiber)

Im Beispiel wurde die Lieferantenkritikalität von 14 und die Bauteilkritikalität von 8 verschiedenen Faktoren beeinflusst. Einen Auszug finden Sie in Bild 2.

Die dargestellte Herangehensweise ermöglicht eine Betrachtung der Risiken innerhalb der Supply Chain aus zwei unterschiedlichen Perspektiven. Diese können je nach Anwendungsfall beliebig definiert werden.

Im Sinne des Projektmanagements hat KBC hierbei folgende Erfolgsfaktoren identifiziert.

LIEFERANTENKRITIKALITÄT	BAUTEILKRITIKALITÄT
<ul style="list-style-type: none"> ♦ Projektmanagement z.B. Erreichbarkeit, Effizienz in der Zusammenarbeit, Projektmanagement-Standards ♦ Management von Sublieferanten z.B. Befähigung, Auditierung, Absicherung gegen Lieferengpässe ♦ Qualitätssicherung z.B. Qualitätsverständnis, Qualitäts-Management-System ♦ Prozessstabilität z.B. Anfälligkeit für Produktionsstillstände, Prozessausschuss ♦ Flexibilität z.B. Reaktionsgeschwindigkeit bei kurzfristiger Stückzahländerung ♦ Etc. 	<ul style="list-style-type: none"> ♦ Anfälligkeit Produktionsverfahren z.B. regelmäßige Ausfälle aufgrund hoher Komplexität ♦ Anforderungen an die Logistik z.B. Empfindlichkeit bei Erschütterung, Feuchtigkeit ♦ Relevanz beim Verbau z.B. Einfluss fehlendes Teil auf Montageprozess ♦ Relevanz für Produktportfolio z.B. Baukastenbauteil ♦ Sicherheitsrelevanz z.B. Auswirkung bei Qualitätsabweichung auf Sicherheit des Endkunden ♦ Etc.

Bild 2: Exemplarische Einflussfaktoren je Risikotreiber im Anwendungsbeispiel

Erfolgsfaktoren für das Projektmanagement in Schritt 1

- Einbindung der zentralen Stakeholder – „Welche Entscheidungsträger sind notwendig, um das Commitment für das Projektvorgehen sicherzustellen?“
- Zweidimensionale Risikobetrachtung – „Welche Dimensionen sind (ggf. in Kombination) für das Risiko tatsächlich ausschlaggebend?“
- Einbindung der relevanten Fachexperten – „Welche Expertenmeinung ist inhaltlich notwendig, um vollständig alle relevanten Einflussfaktoren zu identifizieren?“

Schritt 2: Definition Bewertungslogik

Nach der Identifikation von Risikotreibern und deren Einflussfaktoren werden letztere für jedes mögliche Szenario individuell bewertet. Die bewerteten Einflussfaktoren wiederum sind ausschlaggebend für die Ausprägung der Risikotreiber je bewertetem Szenario.

Grundsätzlich sind hier mehrere Alternativen denkbar, deren Vor- und Nachteile, im Einzelfall abgewogen werden müssen. Exemplarisch kann die Bewertung auf Basis von Schulnoten (1-6), prozentualer Einordnung (0%-100%) oder qualitativer Bewertung (gut, mittel, schlecht) vorgenommen werden. Komplexe Logiken, wie zum Beispiel frei zu vergebende Prozentzahlen von 0%-100% können sinnvoll sein, wenn diese eindeutig bewertbar sind und ein hoher Detailgrad bei der Bewertung erforderlich ist. Bei einer Vielzahl an zu bewertenden Einflussfaktoren und Szenarien kann es jedoch in der Praxis zu einem hohen und gegebenenfalls nicht vertretbaren Aufwand kommen. In solchen Fällen ist eine weniger komplexe Bewertungslogik mit klar definierten und eingeschränkten Bewertungsmöglichkeiten, wie zum Beispiel ein Punktesystem (1-3), zu empfehlen. Auf Basis der bewerteten Einflussfaktoren lässt sich im Anschluss ein Wert berechnen, der die Ausprägung des Risikotreibers je Szenario abbildet (vgl. Schritt 3). Zur Definition der Bewertungslogik zeigt Bild 3 eine schematische Darstellung.

Bei der Berechnung dieser Ausprägung bietet die Methode Spielraum für den Anwender. Neben dem arithmetischen Mittel kann bei Bedarf auch ein gewichteter Mittelwert herangezogen werden. Letzterer ermög-

licht eine individuelle Gewichtung der einzelnen Einflussfaktoren. Dies ist sinnvoll, sobald einzelne Einflussfaktoren das Risiko stärker beeinflussen als andere.

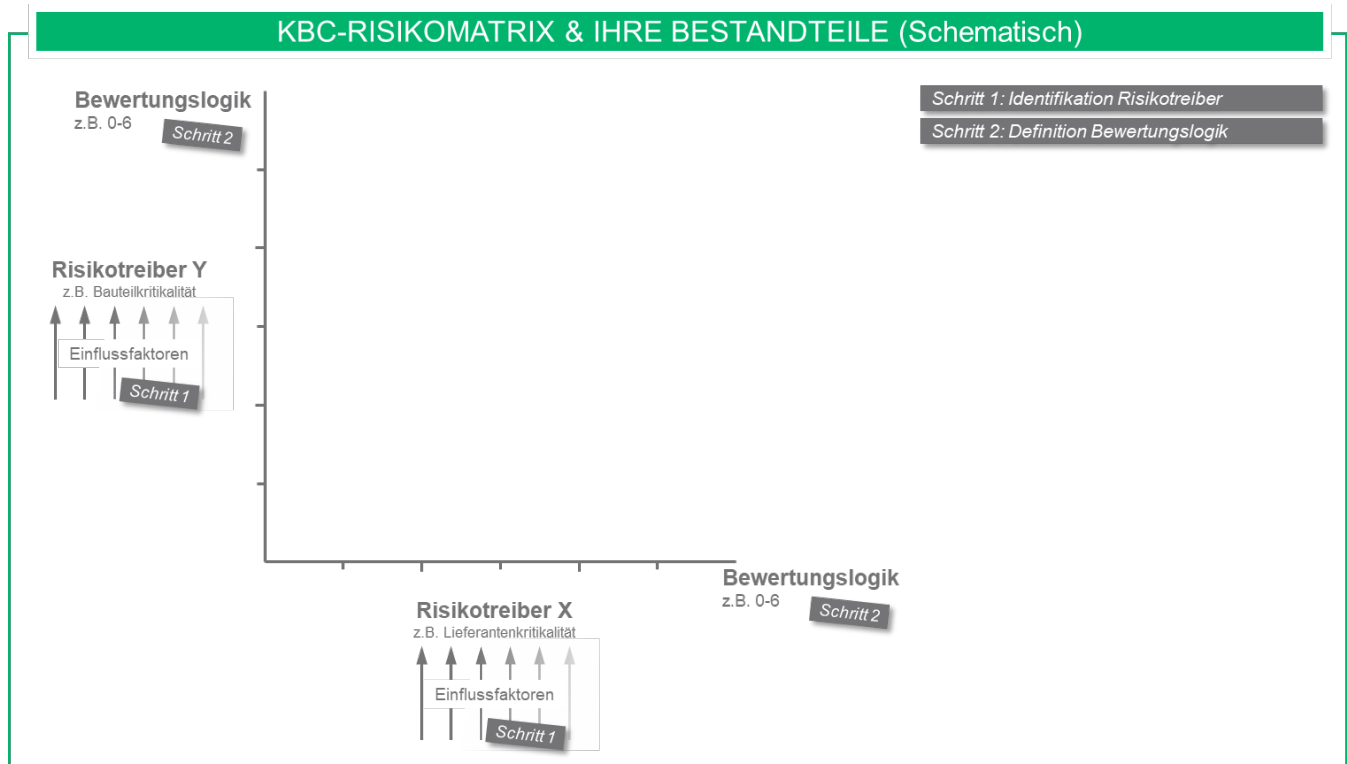


Bild 3: Schematische Darstellung Schritt 2 (Definition Bewertungslogik)

Im konkreten Fall beim Kunden galt es, eine Vielzahl an Einflussfaktoren für zahlreiche Lieferanten (>500) und Bauteile (>150) zu bewerten. Aus diesem Grund wurde eine intuitiv anwendbare Bewertungslogik gewählt. Differenziert wurde zwischen den drei Bewertungsstufen „unkritisch“, „kritisch“ und „sehr kritisch“. Diese wurden in den Zahlenbereich 0,1,2 übersetzt. So konnte für jede der über 600 Lieferanten-Bauteil-Kombinationen das arithmetische Mittel als Lieferanten- bzw. Bauteilkritikalität berechnet werden (vgl. Schritt 3).

Erfolgsfaktoren für das Projektmanagement in Schritt 2

- Eindeutigkeit der Bewertungsstufen – „Wie sind die Bewertungsstufen zu definieren, um eine eindeutige Bewertung sicherzustellen?“
- Detailgenauigkeit der Bewertungslogik – „Welche Bewertungsstufen beschreiben die Risikotreiber realistisch und detailgetreu?“
- Anwendbarkeit der Bewertungslogik – „Wie kann bei der notwendigen Detailgenauigkeit die Anwendbarkeit in der Praxis sichergestellt werden?“ (Berücksichtigung Anzahl und Differenzierbarkeit der Bewertungsstufen, Anzahl mögliche Szenarien etc.)

Schritt 3: Bewertung & Darstellung der Szenarien

Auf Basis der definierten Bewertungslogik erfolgt je Szenario die eigentliche Bewertung sämtlicher Einflussfaktoren. Werden die Einflussfaktoren kritischer bewertet, so steigen die Kritikalitätswerte des betroffenen Risikotreiber. Zur Sicherstellung einer realistischen Einschätzung wird diese durch die jeweils relevanten Experten durchgeführt. Dafür können die zu bewertenden Einflussfaktoren, je nach notwendigem Fachwissen, verschiedenen Organisationseinheiten zugewiesen werden.

Anschließend werden die relevanten Szenarien in einer zweidimensionalen Risikomatrix dargestellt. Die Risikotreiber stellen dabei die beiden Dimensionen der Matrix dar. Die einzelnen Szenarien werden nun entsprechend ihrer Risikotreiber in der Matrix abgetragen.

Im Anwendungsfall wurden unterschiedliche Expertengruppen zur Bewertung der Einflussfaktoren definiert. Beispielsweise führte bei den Lieferanten eine als „sehr kritisch“ bewertete Prozessstabilität zu einem kritischen Ergebnis der Lieferantenkritikalität. Bezüglich der Bauteile hatte z.B. eine kritischere Bewertung der Anfälligkeit des Produktionsverfahrens eine erhöhte Bauteilkritikalität zur Folge. Im KBC Risikomanagement-Tool wurden die Einzelbewertungen (der Einflussfaktoren) aggregiert und die Kritikalitätswerte für Lieferanten und Bauteile automatisiert berechnet. Mithilfe des Tools wurden darauf aufbauend individualisierbare Risikomatrizen zur Darstellung der Lieferanten-Bauteil-Kombinationen erstellt. Somit konnte Transparenz über die identifizierten Risiken in Form von kritischen Lieferanten-Bauteil-Kombinationen hergestellt werden. Bild 4 zeigt eine beispielhafte Risikomatrix, in der Kombinationen mit den höchsten Risiken oben rechts dargestellt werden.

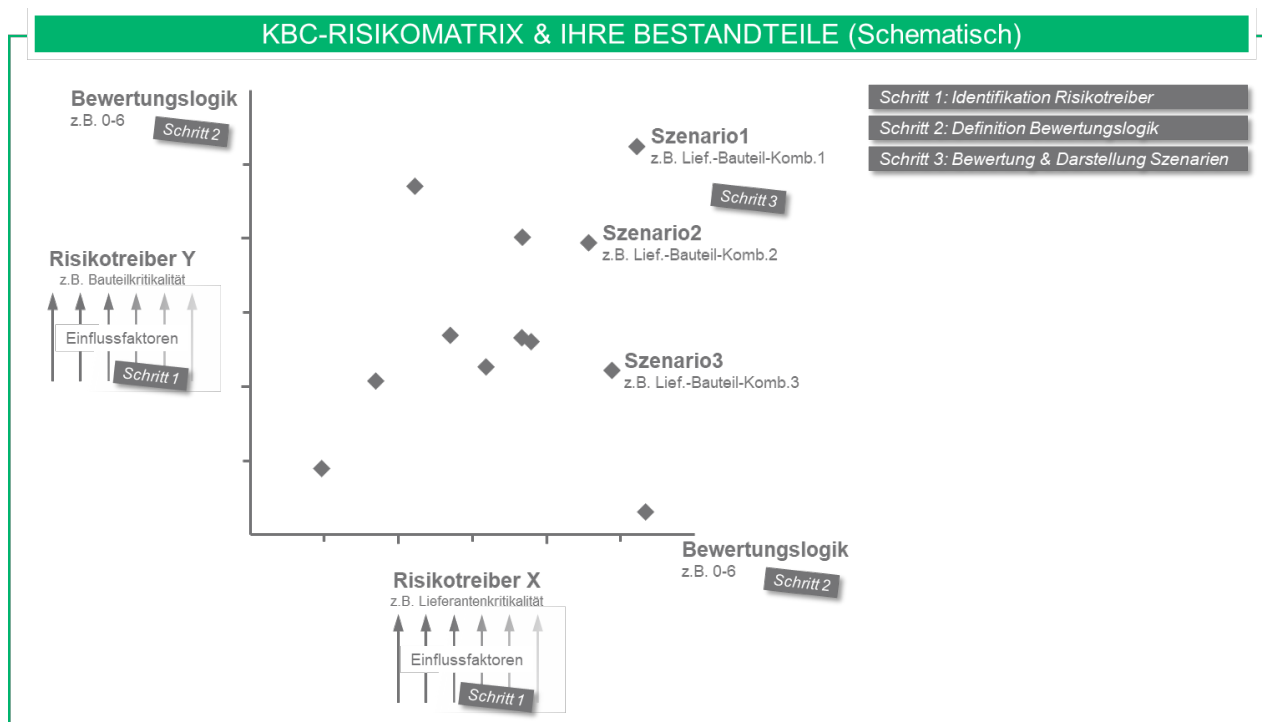


Bild 4: Schematische Darstellung Schritt 3 (Bewertung & Darstellung der Szenarien)

Erfolgsfaktoren für das Projektmanagement in Schritt 3

- Einbindung relevanter Fachexperten – „Welche Expertenmeinung im Unternehmen sichert eine valide Bewertung der Einflussfaktoren?“
- Sicherstellung Vollständigkeit Szenarien – „Sind alle für den Anwendungsfall relevanten Szenarien berücksichtigt und bewertet?“
- Verständlichkeit des Bewertungsprozesses – „Welche Maßnahmen müssen ergriffen werden, um Einfachheit und Unmissverständlichkeit bei der Bewertung sicherzustellen?“ (Anleitung, Schreibschutz in Dokumenten etc.)

Schritt 4: Priorisierung & Maßnahmen

Ziel des letzten Schritts ist es, die gewonnene Transparenz über Risiken in der Supply Chain im Sinne eines zielgerichteten und effizienten Risikomanagements zu nutzen. Dafür ist zunächst eine Priorisierung der Risiken notwendig. Dies gilt insbesondere für komplexe Anwendungsfälle mit umfangreichen Datenmengen, z.B. aufgrund einer Vielzahl an Szenarien. Mithilfe der entwickelten Methode kann die Priorisierung individuell gestaltet werden.

Je nach Anforderung im Projekt können verschiedene Risikogruppen gebildet werden. Beispielsweise ist ein Vorgehen nach dem Pareto-Prinzip möglich. So decken die risikoreichsten Szenarien (20%) den Großteil des Gesamtrisikos (80%) ab. Für die Szenarien je Risikogruppe können dann spezifische Maßnahmen zum zielgerichteten Risikomanagement abgeleitet werden. Damit wird sichergestellt, dass die Intensität der Maßnahmen dem Risikopotenzial der jeweiligen Risikogruppe entspricht. Bild 5 zeigt eine schematische Darstellung zur Priorisierung mithilfe der beschriebenen Risikogruppen.

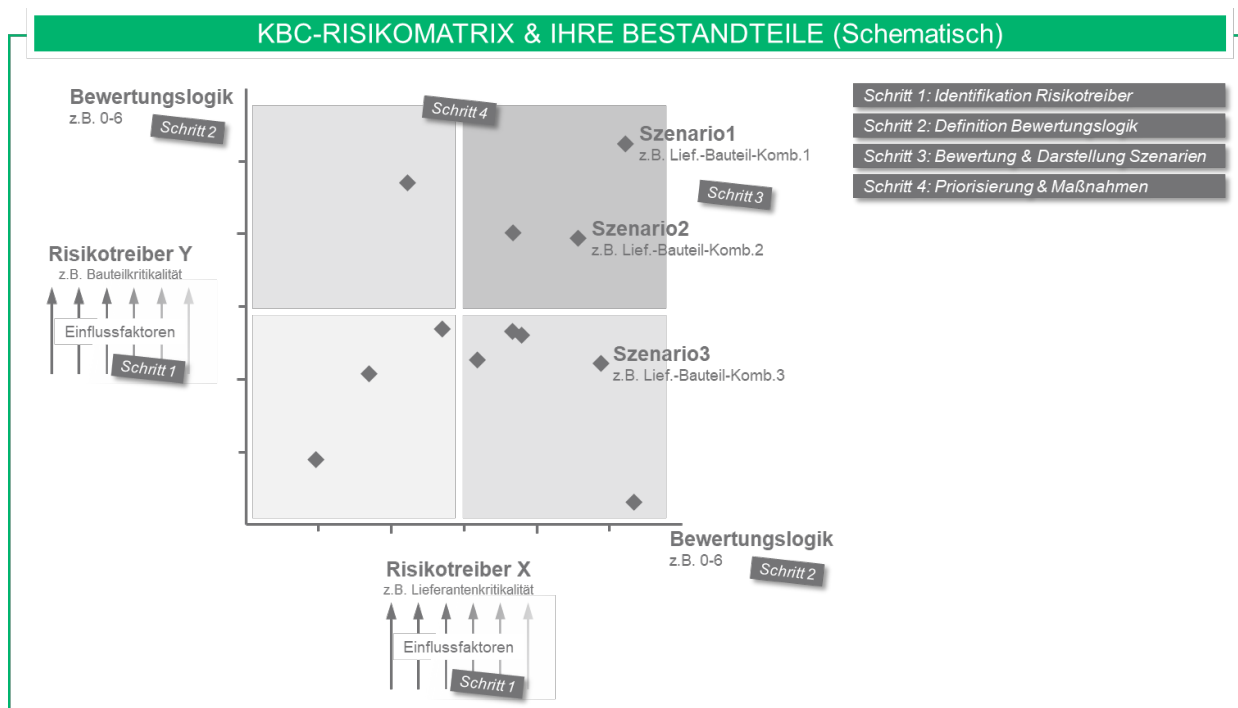


Bild 5: Schematische Darstellung Schritt 4 (Priorisierung & Maßnahmen)

Im KBC Projekt wurde die Priorisierung der Lieferanten-Bauteil-Kombinationen entsprechend der Kundenanforderungen vorgenommen: Der Fokus lag zunächst darauf, Unternehmensrisiken mit direkten negativen Auswirkungen auf den Endkunden zu minimieren. Solche resultieren häufig aus Qualitätsproblemen oder Ausfällen hochkritischer Bauteile. Infolgedessen wurde der Bauteilkritikalität im Verhältnis zur Lieferantenkritikalität ein höheres Gewicht beigemessen. Über das KBC Risikomanagement-Tool wurden die insgesamt über 600 Lieferanten-Bauteil-Kombinationen den kundenspezifischen Risikogruppen zugewiesen. Im Sinne der Übersichtlichkeit wurden diese im Anschluss in separaten Risikomatrizen dargestellt.

Für die einzelnen Risikogruppen wurden jeweils dezidierte Maßnahmenpakete abgeleitet. Diese wurden entsprechend der Bedürfnisse inhaltlich und hinsichtlich des notwendigen Ressourceneinsatzes individuell gestaltet. Die Maßnahmen reichten vom sofortigen Task Force Einsatz bis zu hochspezifischen Einzelmaßnahmen zur Qualitätssicherung beim betroffenen Lieferanten.

Die Risikogruppen mit zugehörigen Maßnahmenplänen ermöglichten dem Kunden eine effiziente Zuordnung der beschränkten finanziellen und personellen Ressourcen. Dadurch erzielte der Kunde eine signifikante Risikoreduzierung. Über regelmäßige Updates der Bewertung von Einflussfaktoren wurde die Risikoreduzierung in Form verbesserter Risikobewertungen sichtbar (vgl. Schritt 3.). Dies hatte eine angepasste Priorisierung der Lieferanten-Bauteil-Kombinationen auf Risikogruppen zur Folge.

Erfolgsfaktoren für das Projektmanagement in Schritt 4

- Dimensionierung Risikogruppen – „Welche eindeutigen und transparenten Grenzen sind zu definieren, um sinnvolle und beherrschbare Risikogruppen zu gewährleisten?“
- Zielgerichtete Maßnahmenableitung – „Welche inhaltlichen Maßnahmen sind notwendig, um bei gegebenen Ressourcen eine maximal mögliche Risikominderung zu erzielen?“
- Sicherstellung Nachhaltigkeit – „Welche Maßnahmen sind notwendig, um die Nachhaltigkeit der Methode im Sinne eines fortlaufenden Risikomanagements in der Supply Chain sicherzustellen?“

Zusammenfassung & Ausblick

Wie beschrieben liegt die Herausforderung des modernen Risikomanagements in Supply Chains im Wesentlichen in der Minimierung von Risiken unter begrenztem Ressourceneinsatz. Diese Aufgabe wird durch die enge Verflechtung meist international agierender Unternehmen in komplexen Lieferantennetzwerken erschwert. Vor diesem Hintergrund wurde eine Methode entwickelt, die eine Identifizierung, Bewertung und Priorisierung von Risiken in der Supply Chain ermöglicht. Auf Basis dieser Priorisierung lässt sich eine effiziente Zuordnung (meist begrenzter) Ressourcen realisieren.

Das von KBC entwickelte Risikomanagement-Tool unterstützt bei der Anwendung der vorgestellten Methode. So werden zunächst die entscheidenden Risikotreiber identifiziert und im Anschluss nach einer klar definierten Systematik bewertet. Darüber hinaus ermöglicht das Tool eine individuell auf die Kundenanforderungen abgestimmte Darstellung und Priorisierung der im Einzelfall relevanten Szenarien. Aufbauend auf die

erfolgte Priorisierung werden Risikogruppen definiert und spezifische Maßnahmenpakete abgeleitet. Im Anwendungsfall konnte so eine nachhaltige Risikominimierung sichergestellt werden konnte. Die Vorteile der Methode sind zusammenfassend in Bild 6 dargestellt.

VORTEILE DER METHODE ZUM RISIKOMANAGEMENT IN DER SUPPLY CHAIN

- ♦ **Einbindung aller relevanten Einflussfaktoren** zur vollständigen Berücksichtigung bestehender Risiken
- ♦ **Reduzierung der Komplexität** im Sinne einer transparenten Darstellung von Risiken in der Supply Chain
- ♦ **Transparente Priorisierung** und eindeutige Zuordnung der Risiken in Risikogruppen
- ♦ **Zielgerichtete Maßnahmenableitung** und effiziente Allokation von finanziellen und personellen Ressourcen
- ♦ **Verankerung der Methode** zur Sicherstellung eines nachhaltigen Risikomanagements in der Supply Chain

Bild 6: Vorteile der Methode zum Risikomanagement in der Supply Chain

Um nach erfolgreicher Einführung der vorgestellten Methode ein kontinuierliches Risikomanagement in der Supply Chain sicherzustellen, ist es sinnvoll, geeignete Schnittstellen zu bestehenden IT-Systemen zu schaffen. Hierüber kann die fortlaufende Aktualisierung der Risikobewertung und angepasste Priorisierung der Lieferanten-Bauteil-Kombinationen ermöglicht bzw. in den Unternehmensprozessen verankert werden. Darüber hinaus kann eine Anreicherung der Risikobewertung durch bestehende KPIs (z.B. Eigenkapitalanteil und Verschuldung, Ausschussquote am Wareneingang) erfolgen, um die Validität der Risikobewertung weiter zu steigern.

Die durch die Anwendung der Methode gewonnene Transparenz stellt für Unternehmen eine wertvolle Datenbasis dar. Neben dem Risikomanagement kann diese in weiteren Organisationseinheiten einen Mehrwert bieten – z.B. beim Benchmarking verschiedener Lieferanten und Technologien (Bauteile) oder bei Vergabe-Entscheidungen für neue Produktumfänge. Die Erfahrung zeigt, dass die vorgestellte Methode neben der Automobilindustrie auch in anderen Branchen, deren Supply Chains ähnlich komplex sind, erfolgreich eingesetzt werden kann.

Literatur

- Bendul und Brüning: Kooperatives Supply Chain Risikomanagement. Neue Wege für den Umgang mit existenzbedrohenden Supply Chain Störungen. Hg. v. Jacob University. Bremen, 2017, S. 5

Verfahren zur Risikoanalyse am Beispiel DESERTEC

Abbildung von Risiken in Großprojekten oder was Risiken und Cocktails gemeinsam haben



Dr. Philipp Gausling

Projektmanager und Experte
für das Risikomanagement von
Großprojekten

Egal ob beim Bahnprojekt Stuttgart 21, der Hamburger Elbphilharmonie oder dem Flughafen Berlin-Brandenburg (BER) – immer wieder kommt es bei Großprojekten zu extremen Abweichungen von der Projektplanung. Für den BER z.B. rechneten die Projektplaner 2006 mit Kosten in Höhe von zwei Milliarden Euro, das Projektende sahen sie für 2011 vor.

Mittlerweile liegen die Kosten bei etwa 6,5 Mrd. Euro und eröffnet wird der Flughafen frühestens 2018 (vgl. Balser/Schneider, 2017). Bei anderen Großprojekten – seien es Schienennetze, Wolkenkratzer oder Kraftwerke – verhält es sich ähnlich: In neun von zehn Großprojekten kommt es zu bedeutenden Planungsabweichungen (vgl. Flyvbjerg, 2014).

Warum bleiben Großprojekte selten in Time & Budget?

Vor diesem Hintergrund drängt sich die Frage auf, warum die Kosten und die Dauer von Großprojekten so schwer einzuschätzen sind. Was treibt die Kosten in die Höhe und warum wird das Projektende so selten eingehalten? Ein in diesem Zusammenhang entscheidender Faktor sind Projektrisiken sowie deren Zusammenspiel: Der Eintritt eines Risikos löst in einer Kettenreaktion häufig weitere Risikoereignisse aus.

Weil Großprojekte überaus komplexe Vorhaben sind, die sich über einen langen Zeitraum erstrecken und viele Stakeholder haben, sind sie mit einer Vielzahl verschiedener Risiken behaftet, die häufig gemeinsam auftreten, auch weil sie sich gegenseitig bedingen: Kommt eine Warenlieferung zu spät (Zuliefererrisiko), verlängert dies oft auch die Projektdauer (Fertigstellungsrisiko). Dadurch werden erst später Einnahmen generiert (Absatzrisiko). Auch Preisschwankungen werden wegen des längeren Projektzeitraums wahrscheinlicher (Preisrisiko). Das Eintreten eines Risikos löst so eine Kettenreaktion aus, während der anderen Risiken eintreten.

Einfluss von Risiken transparent und realitätsnah darstellen

Im vorliegenden Beitrag zeige ich am Beispiel des Wüstenstromprojekts DESERTEC auf, welchen gravierenden Einfluss die Wirkung von Risiken in Großprojekten im Zusammenspiel haben kann und wie wichtig ein realitätsnahes Bild von Risiken ist. Ich stelle in diesem Zusammenhang ein Vorgehen vor, mit dem der Einfluss von Risiken auf das Projektergebnis transparent und realitätsnah dargestellt werden kann und erläutere, was Risiken und Cocktails gemeinsam haben.

Dieser Beitrag richtet sich an alle Initiatoren und Planer von Großprojekten, wie staatliche Institutionen, Unternehmen, Projektleiter oder Projektgesellschaften, sowie an Risikomanager und Interessierte am Risikomanagement von Großprojekten. Ich möchte für den Einfluss von Risiken auf das Projektergebnis sensibilisieren und ein selbstentwickeltes Vorgehen präsentieren, das sich von den bekannten Modellen insofern abhebt, als dass es auch das Zusammenspiel von verschiedenen Risiken in Großprojekten in Businessplänen abbildet (siehe dazu auch den Fachbeitrag "[So schreiben Sie einen Business Case. Teil 4: Sensitivität, Risiko, Empfehlungen](#)", Ausgabe 07/2010)

DESERTEC: Ein interkontinentaler Hoffnungsträger

Ein bekanntes Großprojekt, dem die Vielzahl eintretender Risiken zum Verhängnis wurde, ist das interkontinentale Wüstenstromprojekt DESERTEC, das zwischen 2005 und 2015 für großes Aufsehen sorgte. Das Projekt beinhaltete den Bau vieler Solaranlagen in den Wüsten Nordafrikas und des Mittleren Ostens. Über lange Leitungskorridore sollte ein Teil des Solarstroms schließlich via Hochspannungsgleichstromübertragung in die Bedarfszentren Europas transferiert werden.

Aufgrund seines internationalen Ausmaßes, seiner Komplexität und seines hohen Innovationsgrads war das Projekt besonders vielen Risiken ausgesetzt. Doch der Einfluss simultan auftretender Risiken wurde unterschätzt. Unter anderem führten politische Schwierigkeiten und dynamische Entwicklungen im Energiemarkt schließlich dazu, dass wichtige Partner aus dem mit großen Hoffnungen verbundenen und zunächst als äußerst lukrativ geltende Projekt ausstiegen (siehe dazu "[Wüstenstrom-Projekt Desertec zerfällt](#)", Süddeutsche Zeitung am 14.10.2014).

An Analysen mangelte es nicht...

Verschiedene Institutionen fertigten Wirtschaftlichkeitsanalysen zu diesem Projekt an, wie z.B. das Deutsche Zentrum für Luft- und Raumfahrt (DLR), die DESERTEC Industrial Initiative (DII) und einige Wissenschaftler. Da es jedoch keinen zentral abgesteckten Projektrahmen und keine engen Abstimmungen zwischen den Institutionen gab, gingen alle Analysen von verschiedenen Projektszenarien mit einer unterschiedlichen Anzahl von Solaranlagen, Leitungskorridoren und beteiligten Ländern aus (vgl. Massetti, 2013; Trieb, 2006; Ummel, 2008; Willigst, 2010; Zickfeld, 2013). Die Analysen kamen daher zu deutlich unterschiedlichen Projektbeurteilungen.

... trotzdem kam es zum raschen Aus

Risiken wurden in den Wirtschaftlichkeitsanalysen nur teilweise erfasst. So lag beispielsweise ein starker Fokus auf technische und politische Risiken, wohingegen Zuliefer-, Betriebs- oder Finanzierungsrisiken vernachlässigt wurden. Nicht untersucht wurde der Einfluss von simultan eintretenden Risiken. Mit fatalen Folgen, denn es stellte sich heraus, dass man die Risikosituation unterschätzt hatte: Die als "Arabischer Frühling" bezeichneten politischen Unruhen im mittleren Osten machten den dortigen Bau von Solaranlagen unmöglich, der dynamische Ausbau von erneuerbaren Energien in Europa sorgte dafür, dass das Projekt an wirtschaftlicher Attraktivität verlor und zwischen den Projektbeteiligten kam es während der Projektlaufzeit im Jahr 2014 zu einem Zerwürfnis.

So wandelte sich die anfängliche Euphorie schnell in Ernüchterung. Wären die Risiken im Projekt bereits zu Beginn in Gänze abgebildet worden, wie im folgenden Abschnitt beschrieben, hätte die Situation von Beginn

an realistischer eingeschätzt werden können. Fehlinvestitionen hätten vermieden, oder geeignete Maßnahmen zum Risikomanagement ergriffen werden können.

Abbilden von Risiken

Um Risiken in Businessplänen von Großprojekten richtig abbilden zu können, habe ich das in Bild 1 beschriebene Vorgehen ausgearbeitet (vgl. hier und im gesamten Abschnitt Gausling, 2016). Es basiert auf der führenden internationalen Literatur zum Projektmanagement und kombiniert verschiedene Methoden des Risikomanagements. Dadurch ermöglicht es ein relativ genaues und umfassendes Bild der Risiken in einem Großprojekt. *(Die Ausarbeitung erfolgte im Rahmen der Dissertation des Autors, die 2016 für den deutschen Studienpreis der Körber-Stiftung nominiert wurde, die Redaktion)*

Im Gegensatz zu vielen anderen Verfahren werden bei dieser Vorgehensweise alle Risiken mit ihren Interaktionseffekten erfasst und alle möglichen Projektausgänge mit der jeweiligen Wahrscheinlichkeit dargestellt. Dieses Vorgehen gliedert sich in drei Hauptschritte:

1. Identifizieren unsicherer Inputvariablen
2. Sensitivitätsanalyse
3. simulative Risikoanalyse

Insgesamt besteht das Vorgehen aus 13 Teilschritten, auf die in der folgenden Beschreibung immer wieder Bezug genommen wird.



Bild 1: Empfohlenes Vorgehen zur Abbildung von Risiken in Großprojekten; jeder Hauptschritt besteht aus vier bis fünf Teilschritten.

Schritt 1: Identifikation unsicherer Inputvariablen

Bei der Projektkalkulation sollten Sie zunächst zwischen sicheren und unsicheren Inputvariablen unterscheiden (vgl. Gausling, 2016; Werthschulte, 2005). Während sichere Inputvariablen genau einen Wert annehmen können (z. B. der Körperschaftssteuersatz, sofern ein stabiles Regierungsumfeld vorliegt), kann bei unsicheren Inputvariablen der Wert schwanken (z.B. der Preis für Stahl). Das Identifizieren unsicherer Inputvariablen ist deswegen so wichtig, weil Sie deren Unsicherheit später in der Projektkalkulation darstellen müssen, um die Unsicherheit der Zielgröße ermitteln zu können.

Inputvariablen und Zielgröße

Inputvariablen sind Parameter wie z.B. der Absatzpreis, die Materialkosten oder die Fertigungskosten, die Sie für die Berechnung der definierten Zielgrößen eines Projekts, wie beispielsweise des Kapitalwerts, benötigen. Je nach Projekt spielen unterschiedliche Inputvariablen eine Rolle: Während bei dem Bau einer Solaranlage beispielsweise die Einstrahlungswerte zur Berechnung der Rentabilität des Projekts von Bedeutung sind, können diese beim Bau eines Schienennetzes komplett vernachlässigt werden. Die Inputvariablen müssen Sie also zu einem großen Teil für das jeweilige Projekt neu bestimmen.

Beim Aufstellen eines Businessplans wird jeder Inputvariablen zunächst ein Wert zugeordnet. Der Stahlpreis z.B. erhält den Wert 300 Euro pro Tonne. In der Praxis kann der Wert einer Inputvariablen jedoch nur sehr selten mit vollständiger Sicherheit vorausgesagt werden. Bezogen auf den Stahlpreis ist u.a. nicht klar, wie sich Materialpreise, Wechselkurse oder die Absatzmenge entwickeln und dadurch der Preis von der ursprünglichen Planung abweicht, die häufig auf einer Schätzung beruht. Daher ist es wichtig, zwischen sicheren Inputvariablen mit genau einem Wert und unsicheren Inputvariablen mit möglichen Wertschwankungen zu unterscheiden.

Welche Variablen werden von Risiken beeinflusst?

Als Erstes sollten Sie daher bestimmen, welche Inputvariablen von Risiken beeinflusst werden und somit im Rahmen der Projektkalkulation verschiedene Werte annehmen können. Für ein systematisches Vorgehen empfiehlt es sich, zunächst alle Inputvariablen (*Teilschritt 1*) und alle Risikoarten (*Teilschritt 2*) aufzulisten. Je größer und komplexer das Projekt ist, desto mehr Inputvariablen und Risiken spielen in der Regel eine Rolle.

Um schließlich Zusammenhänge zwischen Inputvariablen und Risikoarten aufzuzeigen, sollten Sie die Risikoarten den Inputvariablen in einer Zusammenhangsmatrix gegenüberzustellen (*Teilschritt 3*, siehe Tabelle 1) (vgl. hier und im Folgenden Gausling, 2016; Pollio, 1999; Werthschulte, 2005). Die Zusammenhänge zwischen den Risikoarten und Inputvariablen lassen sich durch sachlogische Überlegungen projektspezifisch erschließen.

Inputvariablen	Risikoarten							Einstufung
	Technik	Fertigstellung	Betrieb	Management	Markt	Länder	usw.	
(Absatz-)Preis					•	•		Unsicher
(Absatz-)Menge	•	•	•	•	•	•		Unsicher
Investitionsauszahlungen	•	•						Unsicher
Körperschaftssteuersatz						(•)		Sicher
Fremdkapitalzinssatz						•		Unsicher
Projektdauer		•				•		Unsicher
Technologie								Sicher
usw.								

Tabelle 1: Beispielhafte Zusammenhangsmatrix (Ausschnitt) zwischen Inputvariablen und Risikoarten

Quelle: eigene Darstellung in Anlehnung an Gausling, 2016; Pollio, 1999; Wertschulte, 2005).

Unsichere und sichere Inputvariablen

Anschließend können Sie die unsicheren Inputvariablen identifizieren (*Teilschritt 4*). Eine Variable gilt als **unsicher**, wenn sie von einem oder mehreren Risiken beeinflusst wird. Der für sie geschätzte Wert kann je nach Eintrittswahrscheinlichkeit und Schadensausmaß der beeinflussenden Risiken stark schwanken.

Der Absatzpreis (Tabelle 1) unterliegt z.B. stark dem Marktrisiko sowie dem Länderrisiko: Der zuvor prognostizierte Absatzpreis kann zum einen aufgrund großer und neuer Konkurrenz (Marktrisiko) oder zum anderen aufgrund einer höheren staatlichen Besteuerung (Länderrisiko) nicht mehr am Markt erzielt werden.

Wird eine Inputvariable von keiner Risikoart beeinflusst, gilt sie als **sichere Variable**, bei der die Projektplaner keine Abweichungen vom zugrunde gelegten Wert erwarten. Der Körperschaftssteuersatz oder die Wahl der Technologie unterliegen im vorliegenden Fall z.B. keinem speziellen Risiko und gelten als sicher gegeben.

Nächste Schritte zur Risikoanalyse

Bei der Projektkalkulation sollten Sie somit berücksichtigen, dass eine Inputvariable aufgrund von Risiken verschiedene Werte annehmen kann. Nach der Identifikation der unsicheren Inputvariablen geht es darum, die Mehrwertigkeit dieser Inputvariablen entsprechend abzubilden. Dazu bestehen verschiedene Methoden wie z.B. die Sensitivitätsanalyse und die simulative Risikoanalyse (vgl. Tytko, 1999).

Während die Sensitivitätsanalyse den Einfluss der unsicheren Inputvariablen auf das Projektergebnis isoliert betrachtet, berücksichtigt die etwas aufwändigere simulative Risikoanalyse den Einfluss aller unsicheren Inputvariablen und ihrer Wechselwirkungen simultan. Obwohl die simulative Risikoanalyse ein deutlich realitätsnäheres Bild der Risikosituation ermöglicht, empfiehlt es sich, mit einer Sensitivitätsanalyse zu beginnen: Dadurch können Sie Inputvariablen mit einem geringen Einfluss auf das Projektergebnis ausschließen und damit den Aufwand bei der simulativen Risikoanalyse verringern.

Schritt 2: Sensitivitätsanalyse

Die Sensitivitätsanalyse zeigt, welchen Einfluss die Veränderung des Werts einer einzelnen Inputvariable auf das Projektergebnis hat (vgl. hier und im Folgenden Reuter, 2010). Dazu variieren Sie den Wert einer einzelnen unsicheren Inputvariable (*Teilschritt 5*). Anschließend können Sie die Wirkung dieser Veränderung auf die Zielgröße näher betrachten (*Teilschritt 6*). Auf diese Weise können Sie feststellen, auf welche Inputvariablen das Projektergebnis besonders sensibel reagiert (*Teilschritt 7*).

Verändern Sie jeweils nur den Wert einer einzelnen Inputvariablen, damit Sie die Veränderung des Projektergebnisses genau auf diese Variable zurückführen können. Inputvariablen mit einem geringen Einfluss auf das Projektergebnis können Sie in der weiteren Risikoanalyse vernachlässigen, um den Aufwand der weiteren Risikoanalyse zu reduzieren (*Teilschritt 8*).

Beispiel: Je stärker sich die Erhöhung des Materialpreises auf das Projektergebnis auswirkt, desto größer ist die **Sensitivität** dieser Inputvariablen. Reagiert das Projektergebnis kaum auf den Materialpreis, können Sie diese Inputvariable anschließend vernachlässigen.

Sensitivitätsanalysen lassen einen direkten Rückschluss auf die Wirkungsbeziehung zwischen den Inputvariablen und der Zielgröße bzw. den Zielgrößen zu. Sie ermöglichen zudem erste Aussagen über Schwankungen des Projektergebnisses. Außerdem kann man sie relativ schnell und kostengünstig durchführen. In der Praxis werden daher oft ausschließlich Sensitivitätsanalysen durchgeführt (vgl. Flyvbjerg, 2002).

Grenzen der Sensitivitätsanalyse

Ein solches Vorgehen allein reicht allerdings nicht aus, denn die Sensitivitätsanalyse hat einen großen Nachteil: Sie ermöglicht keine Aussage darüber, **mit welcher Wahrscheinlichkeit eine Veränderung des Werts der Inputvariablen eintritt**.

Zudem bildet die Sensitivitätsanalyse keine Wechselbeziehungen zwischen Risiken sowie zwischen verschiedenen Inputvariablen ab. So wird in einer Sensitivitätsanalyse der Einkaufspreis als Inputvariable variiert, um den isolierten Effekt des Marktrisikos auf das Projektergebnis zu testen. Es kann jedoch sein, dass sich aufgrund verspäteter Lieferungen (Zulieferrisiko) die Projektdauer verlängert (Fertigstellungsrisiko) und dadurch wieder die Prognose für die Materialpreise unsicherer wird, weil sie weiter in die Zukunft reicht (Marktrisiko). Diese Wechselbeziehungen können das mögliche Ergebnisspektrum der Projektzielgrößen stark beeinflussen und sollten daher einen zentralen Teil jeder Risikoanalyse darstellen.

Trotz dieser Nachteile lohnt sich das Durchführen einer Sensitivitätsanalyse. Denn sie vermittelt einerseits einen ersten Eindruck davon, wie stark das Projektergebnis von den einzelnen Inputvariablen abhängt. Andererseits gibt sie einen Überblick darüber, auf welche Inputvariablen das Projektergebnis stark reagiert und ermöglicht somit eine Vorauswahl besonders sensibler Inputvariablen.

Schritt 3: Simulative Risikoanalyse

Nun unterziehen Sie die sensitiven Inputvariablen einer simulativen Risikoanalyse (vgl. hier und im Folgenden Gausling, 2016, Werthschulte, 2005). Dazu verändern Sie – im Gegensatz zur Sensitivitätsanalyse – sämtliche relevanten Inputvariablen simultan, und berücksichtigen die Wechselwirkungen zwischen den Variablen.

Die Werte der Inputvariablen wählen Sie dabei zufällig aus, basierend auf einer für sie aufgestellten Wahrscheinlichkeitsverteilung und ihrer Wechselbeziehungen. Die Werte werden immer wieder auf Basis ihrer Wahrscheinlichkeit und Wechselbeziehungen simultan verändert.

Monte-Carlo-Simulation

Als gängigstes Verfahren der simulativen Risikosimulation gilt die Monte-Carlo-Simulation (vgl. Gleißner, 2004). Bei dieser Art der Simulation werden die Werte der Inputvariablen zufallsbedingt immer wieder neu ermittelt. Für jede Wertkombination der Inputvariablen wird die Zielgröße wieder neu kalkuliert. Bei vielen Wiederholungen mit geeigneter Software ergibt sich schließlich ein realistisches Bild darüber, welche möglichen Ergebnisse die Zielgröße annehmen kann und mit welcher Wahrscheinlichkeit die jeweiligen Ergebnisse eintreten. Es wird somit transparent, welchen Einfluss das Zusammenwirken der Risiken im Projekt auf das Projektergebnis haben kann.

In der Praxis gehen Sie dazu am besten so vor: Bestimmen Sie zunächst die möglichen Werte der Inputvariablen zusammen mit der Wahrscheinlichkeit ihres Auftretens. Dafür können Sie entweder historische Daten heranziehen oder Experten um ihre Einschätzung bitten. Da Großprojekte sehr individuell beschaffen sind, liegen oft keine historischen Daten zur Verteilung der Werte der Inputvariablen vor. Es empfiehlt sich also eine Einschätzung durch Experten.

Auswahl der Experten

Als Experten wählen Sie am besten eine Person, die sich nicht nur sehr gut mit dem Projekt auskennt, sondern auch über hohe fachliche Expertise im Hinblick auf die betrachteten Inputvariablen und Risiken verfügt. Geht es beispielsweise um die Inputvariable "Fremdkapitalzins", können wahrscheinlich Fremdkapitalgeber die beste Einschätzung über mögliche Schwankungen geben. Ist die Inputvariable hingegen der Stahlpreis, eignet sich z.B. ein erfahrener Einkäufer aus dem Unternehmen, das für die Stahlbeschaffung innerhalb des Projekts zuständig ist, um mögliche Preisschwankungen einzuschätzen.

Ich empfehle, die Unsicherheit einer Inputvariablen wenn möglich durch mindestens zwei Experten einzuschätzen. Sollten Sie das Gefühl haben, die Einschätzungen der beiden Experten liegen weit auseinander, ziehen Sie am besten einen dritten Experten zu Rate, um die Einschätzungen der anderen Experten zu validieren.

Da es sehr schwer ist, eine Verteilung für eine Inputvariable aufgrund der diversen Risikoeinflüsse und der dadurch bedingten Vielzahl an möglichen Verteilungswerten genau zu schätzen, empfiehlt sich folgendes Vorgehen: Zunächst sollten alle Risikoarten im Hinblick auf ihre Eintrittswahrscheinlichkeit und ihr Schadensausmaß für das Projekt durch Experten eingeschätzt werden (*Teilschritt 9*). Danach sollten die Experten eine **Dreipunktschätzung** zu den möglichen Werten der Inputvariablen abgeben (*Teilschritt 10*).

Dreipunktschätzung

Bei der Dreipunktschätzung betrachten Sie die einzelnen Inputvariablen zusammen mit den entsprechenden Risiken (vgl. Gausling, 2016; Kanacher, 2010; Johnson, 1999). Auf Grundlage der vorherigen Abschätzung des Schadensausmaßes und der Eintrittswahrscheinlichkeit der Risikoarten sollten die Experten nun in der Lage sein, den pessimistischen, den optimistischen und den wahrscheinlichsten Wert einer Inputvariablen zu schätzen. Mithilfe dieser drei Werte können Sie nun eine Dreiecksverteilung für die unsichere Inputvariable aufstellen (*Teilschritt 11*). So sollten Sie bei jeder unsicheren Inputvariable vorgehen.

Beispiel: Nehmen wir an, der Preis für Stahl liegt bei 300 Euro pro Tonne. Durch sachlogische Überlegung im Rahmen der Zusammenhangsmatrix wird klar (*Teilschritt 1-4*), dass das Marktrisiko den Preis bestimmt. Aus den Sensitivitätsanalysen geht hervor, dass der Preis für Stahl das Projektergebnis wesentlich beeinflussen kann (*Teilschritt 5-8*). Der Experte, in diesem Fall ein langjähriger Einkäufer, schätzt auf Basis seiner Erfahrung in der Stahlindustrie, dass ein Marktrisiko zu 80% eintritt (*Teilschritt 9*).

Für diesen Fall geht er von starken Schwankungen um die 50% nach oben und 30% nach unten aus. Der Preis kann somit zu 40% ($50\% \times 80\%$) nach oben oder zu 24% ($30\% \times 80\%$) nach unten abweichen. Somit kann er nun einen pessimistischen Wert von 228 Euro/t [$300 \text{ Euro/t} - 72 \text{ Euro/t}$ (24% von 300 Euro/t)], einen wahrscheinlichen Wert von 300 Euro/t und einen optimistischen Wert von 450 Euro/t [$300 \text{ Euro/t} + 150 \text{ Euro/t}$ (50% von 300 Euro/t)] annehmen (*Teilschritt 10*). Daraus ergibt sich die in Bild 2 dargestellte Dreiecksverteilung.

An dieser Stelle sei anzumerken, dass die Dreiecksverteilung nicht die tatsächliche Verteilung der Inputvariablen widerspiegelt. Empirische Studien belegen jedoch, dass diese Verteilung der realen Verteilung meistens sehr nahe kommt und sowohl vom Aufwand als auch von der Komplexität her deutlich einfacher einzuschätzen ist, als für die reale Verteilung die Wahrscheinlichkeit jedes Werts einzeln zu bestimmen (vgl. Gausling, 2016; Johnson, 1999). Daher wird sie in der Praxis häufig verwendet.

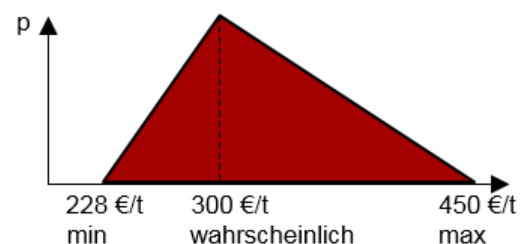


Bild 2: Beispiel für eine Dreiecksverteilung des Stahlpreises.

Vorsicht bei Meta-Unsicherheit

Die Expertenschätzung birgt eine zusätzliche Unsicherheit: Sie ist subjektiv. Zwei Experten können für eine Variable zu ganz unterschiedlichen Risikoeinschätzungen kommen. Diese Meta-Unsicherheit bzw. Unsicherheit über die Unsicherheit ist ein zusätzliches Indiz dafür, dass das Projektergebnis mit großer Unsicherheit behaftet ist und sollte daher abgebildet werden (vgl. Pritsch, 2000).

Um die Meta-Unsicherheit in der Dreiecksverteilung der Inputvariablen abzubilden, können Sie im Rahmen der Dreipunktschätzung beispielsweise den optimistischsten Wert der optimistischen Experteneinschätzungen, den pessimistischsten Wert der pessimistischen Experteneinschätzungen und einen Durchschnitt der wahrscheinlichsten Experteneinschätzung als wahrscheinlichsten Wert annehmen.

Qualitative Risiken

Ein großer Vorteil der Dreipunktschätzung besteht darin, dass auch qualitative Risiken wie z.B. politische Risiken und ihre quantitative Bedeutung für den Wert der Inputvariablen durch die Experten eingeschätzt werden können. Somit können auch qualitative Risiken in der Schätzung quantitativ abgebildet werden. Zudem kann das Zusammenwirken von Risiken und ihre Auswirkung auf die Inputvariablen implizit berücksichtigt werden.

Beispiel: Die Dauer eines Projekts kann sich durch eine verspätete Zulieferung (Zulieferrisiko) oder durch unvorhergesehene Konstruktionsschwierigkeiten (technisches Risiko) verzögern. Der Experte schätzt ein, wie sich die Projektdauer beim Eintritt aller Risiken im optimistischen, pessimistischen und wahrscheinlichsten Fall verändern könnte und impliziert damit mögliche Interaktionseffekte der Risikoarten. Auch qualitative Einflüsse wie z.B. politische Unruhen, die eintreffen könnten (politische Risiken), kann er in sein Kalkül miteinbeziehen und somit messbar machen.

Als nächstes sollten die Experten die Abhängigkeiten der Inputvariablen einschätzen (*Teilschritt 12*). Die Abhängigkeiten können Sie über den sogenannten Rangkorrelationskoeffizienten (RKK) nach Spearman erfassen (vgl. Werthschulte, 2005). Mit dessen Hilfe können Sie feststellen, ob die Inputvariablen stark ($RKK = 0,9$), schwach ($RKK = 0,5$) oder gar nicht ($RKK = 0$) voneinander abhängen.

Beispiel: Steigt der Fremdkapitalzinssatz, steigen in der Regel auch die Investitionsauszahlungen. Hier können Sie einen schwachen Zusammenhang annehmen ($RKK = 0,5$). Der Stromabnahmepreis jedoch bleibt davon unberührt, der RKK beträgt null.

Schätzen Sie den RKK für alle Beziehungen der Inputvariablen. Die Werte können Sie anschließend in einer sogenannten Korrelationsmatrix eintragen. Wenig realistische Wertkombinationen (z.B. der Fremdkapitalzins steigt, aber die Investitionsauszahlungen sinken) können Sie dadurch von der Simulation ausschließen.

Anschließend können Sie die simulative Risikoanalyse via Monte-Carlo-Simulation durchführen (*Teilschritt 13*). Bei der Monte-Carlo-Simulation werden für alle Inputvariablen zufällige Werte gemäß der Dreiecksverteilung (aus Teilschritt 9-11) und der gegenseitigen Abhängigkeiten der Inputvariablen (aus Teilschritt 12) simuliert. Führen Sie anhand dieser Werte die Projektkalkulation durch. Wiederholen Sie den Vorgang mehrmals (z.B. 100.000 Mal). Das sollte mit moderner Technologie lediglich ein paar Minuten dauern.

Dabei erhalten Sie immer wieder neue Werte für Ihre Zielgröße, bis sich schließlich ein realistisches Bild möglicher Ergebnisse und ihrer Eintrittswahrscheinlichkeit ergibt. Ein geeignetes Programm für eine simulative Risikoanalyse ist die EXCEL-basierte Anwendung Oracle Crystal Ball. Einen Gesamtüberblick über das hier beschriebene methodische Vorgehen zum Abbilden von Risiken gibt Bild 3.

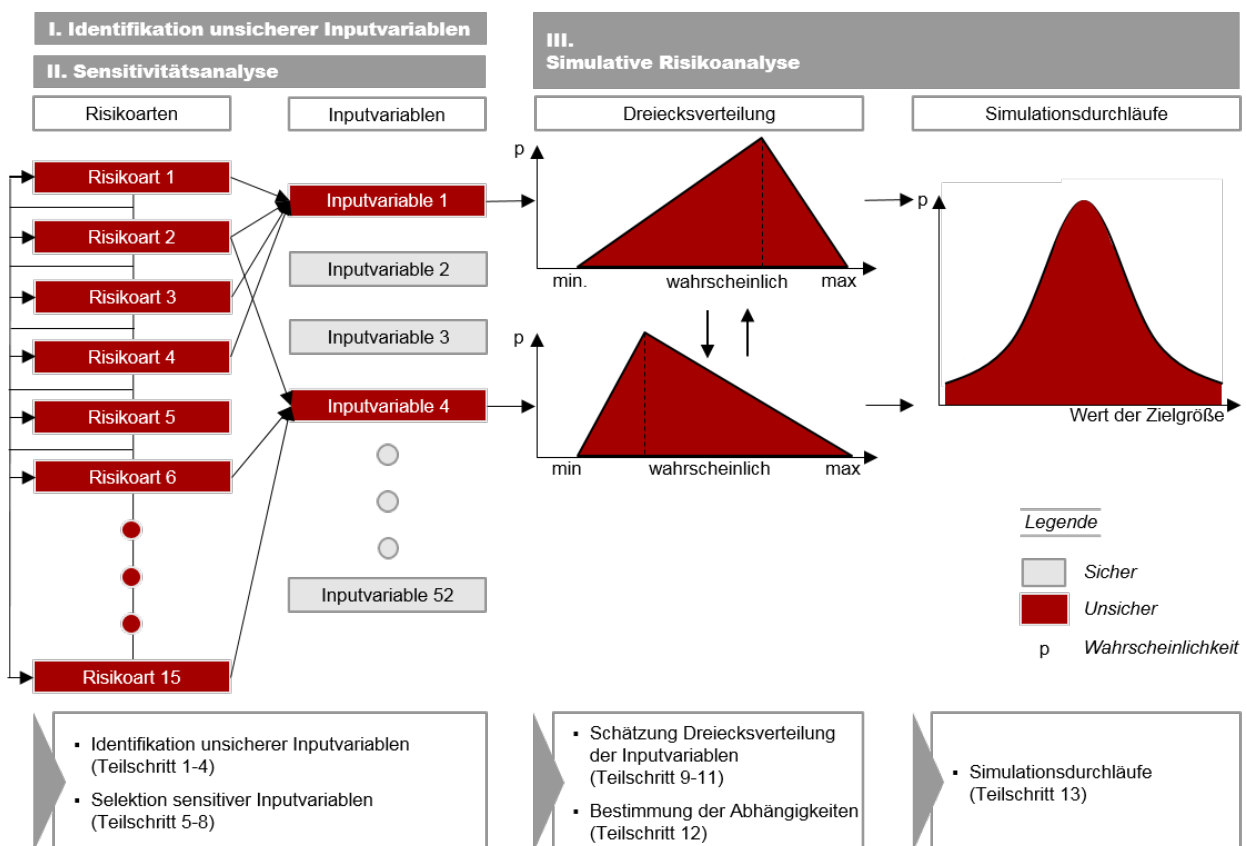


Bild 3: Methodische Beschreibung des Vorgehens bei der Risikoanalyse. (Quelle: eigene Darstellung in Anlehnung an Gausling, 2016)

Warum das Abbilden von Risiken so wichtig ist und was Risiken mit Cocktails zu tun haben

Den Nutzen einer sauberen Abbildung von Projektrisiken will ich im Folgenden am Beispiel DESERTEC verdeutlichen. Dieses riesige interkontinentale Solarstrom- und Infrastrukturprojekt eignet sich besonders gut zur Darstellung von Projektrisiken und ihres Einflusses auf das Projektergebnis, da es unter anderem wegen seines internationalen Ausmaßes, seines langen Projektzeitraums und seiner technischen sowie organisatorischen Komplexität mit sehr vielen Risiken behaftet war (vgl. hier und im gesamten Abschnitt Gausling, 2016).

Das Beispiel DESERTEC – Bewertung unter Berücksichtigung der Risiken

In den Wüsten Nordafrikas und des Mittleren Ostens sollte eine Vielzahl von thermischen Solarkraftwerken konstruiert werden und die elektronische Energie zum Teil über riesige Leitungskorridore via Hochspannungsgleichstrom nach Europa transferiert werden. An diesem Projekt waren sehr viele verschiedene Unternehmen aus mehreren Ländern beteiligt, darunter namhafte Unternehmen wie Bosch, Siemens, RWE, Schott Solar, die Deutsche Bank oder die Münchener Rück.

Drei Leitungskorridore

Da unter dem Namen DESERTEC viele unterschiedliche Projektszenarien entworfen wurden, gehen wir zur Vereinfachung im Folgenden von einem Projektszenario mit drei Leitungskorridoren aus, welche ich aufgrund ihrer ausgereiften Planung und ihres unterschiedlichen Risikoprofils ausgewählt habe: Ein Leitungskorridor von Marokko nach Deutschland, ein Leitungskorridor von Tunesien nach Italien und ein Leitungskorridor von Ägypten nach Bulgarien.

Die installierte Gigawatt-Zahl pro Leitungskorridor beträgt 11,4, also insgesamt 34,2 GW. Das Projekt beginnt 2010 und soll 2050 enden (für weitere Ausführungen vgl. Gausling, 2016). Für diese Leitungen besteht dank den bereits erwähnten Wirtschaftlichkeitsanalysen eine besonders gute Datengrundlage, zudem repräsentieren sie eindrucksvoll das interkontinentale Ausmaß des Projekts.

Betrachtung aus Investorensicht

Zur Vereinfachung bewerte ich das Projekt allein aus Investorensicht, daher bewerte ich das Projekt rein nach dem Kapitalwert. Normalerweise ist in Großprojekten nicht nur die Entscheidung der Investoren, sondern auch die Bewertung anderer Projektbeteiligter wie Finanzdienstleister oder staatlicher Institutionen relevant, sodass auch andere Zielgrößen betrachtet werden müssen, wie z.B. der Schuldendienstdeckungsgrad für Kreditgeber oder die Subventionshöhe aus Sicht des Staates.

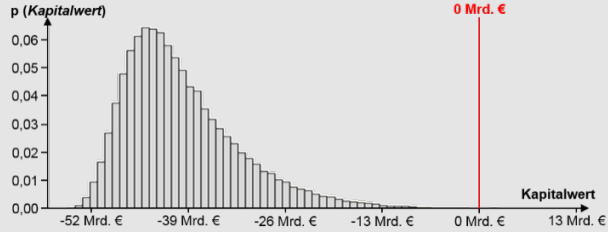
Bewertung	Ohne Risiko	Mit Risiko (Sensitivitätsanalyse)	Mit Risiko (Simulative Risikoanalyse)	
Beschreibung	Inputvariablen haben genau einen Wert	Veränderung des Werts einer einzelnen unsicheren Inputvariablen	Simultane Veränderung der Werte aller unsicheren Inputvariablen Simulation vieler Wertkombinationen basierend auf Zufall Darstellung des Ergebnisspektrums mit Wahrscheinlichkeiten	
Beispiel Kapitalwert im Großprojekt DESERTEC	35 Mrd. Euro	13 Mrd., wenn die Projektdauer um 20% steigt 25 Mrd., wenn der Strompreis um 20% sinkt (weitere Inputvariablen analog)	Durchschnitt Standardabweichung	ca. - 40 Mrd. Euro ca. 8 Mrd. Euro
				
Projekt- beurteilung	Das Projekt ist attraktiv, da der Kapitalwert positiv ist.	Der Kapitalwert kann bei der Veränderung des Wertes einzelner Inputvariablen stark schwanken. Der Kapitalwert bleibt aber selbst bei 20-prozentigen Änderungen noch positiv. Das Projekt bleibt attraktiv.	Das Projekt ist extrem unattraktiv, da der Kapitalwert im Mittel bei - 40 Mrd. Euro und damit deutlich im negativen Bereich liegt und mit einer Standardabweichung von 8 Mrd. Euro stark schwankt. Zudem ist der Kapitalwert in über 99% der Fälle negativ.	

Tabelle 2: Einfluss der Berücksichtigung von Risiken auf die Investitionsentscheidung am Beispiel DESERTEC.

(Quelle: eigene Darstellung in Anlehnung an Gausling, 2016)

Tabelle 2 zeigt den Kapitalwert in Abhängigkeit unterschiedlicher Methoden zur Risikobewertung für das Beispiel DESERTEC. Bei der *Betrachtung ohne Risiken* sieht das Projekt äußerst attraktiv für Investoren aus: Der Kapitalwert liegt bei ca. 35 Mrd. Euro.

Unter *Berücksichtigung von Risiken* verändert sich die Entscheidungssituation jedoch. Nach der Durchführung von *Sensitivitätsanalysen* wirkt das Projekt weniger attraktiv, wird aber weiterhin positiv bewertet. Verlängert sich beispielsweise die Projektdauer um 20%, sinkt der Kapitalwert auf 13 Mrd. Euro. Wird der Stromabnahmepreis um 20% verringert, fällt der Kapitalwert ebenfalls deutlich (auf 25 Mrd. Euro). Der Kapitalwert bleibt allerdings selbst bei einer 20%-igen Wertschwankung einzelner Inputvariablen positiv. Das Projekt ist somit selbst durch starke risikobedingte Schwankungen nicht gefährdet und bleibt weiterhin attraktiv.

Der Cocktail-Effekt

Eine grundlegend neue Situation ergibt sich hingegen bei der simultanen Berücksichtigung aller Risiken und möglicher Interaktionseffekte mittels einer simulativen Risikoanalyse. Für diese Analyse habe ich die Risiken von mehreren Experten aus unterschiedlichen Fachbereichen und Unternehmen, die sich auch beruflich mehrere Jahre mit dem DESERTEC-Projekt beschäftigt haben, bewerten lassen.

Auf Grundlage dieser Bewertung wurden die Verteilungen der Werte der Inputvariablen mittels Dreipunktschätzung festgelegt und eine Monte-Carlo-Simulation durchgeführt. Dieser Analyse zufolge ist das Projekt hochgradig unattraktiv. Der Einfluss der Risiken führt dazu, dass das Projekt im Durchschnitt bei einem Kapitalwert von -40 Mrd. Euro liegt und in über 99% der Fälle einen negativen Kapitalwert annimmt.

Diesen Effekt bezeichne ich als "Cocktail-Effekt". Für einen Cocktail werden in der Regel mehrere Spirituosen zusammen mit süßen Flüssigkeiten gemischt. Das macht es schwer, den Alkoholanteil im Getränk richtig einzuschätzen. Die explosive Wirkung ergibt sich aus dem Zusammenspiel der verschiedenen Stoffe. So verhält es sich auch mit Risiken in einem Projekt.

Vor allem bei einem Großprojekt fällt es aufgrund der vielen verschiedenen Risikoarten oft schwer, ihre Wirkung richtig einzuschätzen. Im Zusammenwirken können die Risiken eine explosive Wirkung entfalten und das Projektergebnis erheblich beeinflussen. Das heißt, je mehr Risiken zusammenkommen, desto stärker kann das Projekt später von der ursprünglichen Planung abweichen. Mit Risiken ist es also wie in einem Cocktail. Je komplexer das Projekt ist und je mehr Risiken zusammenkommen, desto stärker kann es später "knallen". Aufgrund des Cocktail-Effekts ist es wichtig, dass die Risiken in ihrem Zusammenspiel in Großprojekten abgebildet werden.

Fazit

Ziel dieses Artikels war die Darstellung eines Vorgehens, mit dem Risiken in Großprojekten mitsamt ihren Interaktionseffekten adäquat in Businessplänen abgebildet werden können. Das Beispiel des Solastromprojekts DESERTEC sollte dabei veranschaulichen, was für einen gewaltigen Einfluss das Zusammenspiel von Risiken in Großprojekten auf das Projektergebnis hat, wie wichtig die richtige Darstellung der Risiken dabei ist und was Risiken und Cocktails gemeinsam haben.

Um Risiken in Großprojekten richtig abzubilden, schlage ich ein Dreischritt-Verfahren vor: Zunächst sollten Sie die unsicheren Inputvariablen des Kalkulationsmodells identifizieren. Unterziehen Sie daraufhin alle unsicheren Inputvariablen eine Sensitivitätsanalyse, um die Inputvariablen mit einem geringen Einfluss auf das Projektergebnis aus der weiteren Risikoanalyse zu eliminieren. Anschließend können Sie mithilfe einer Monte-Carlo-Simulation eine simulative Risikoanalyse durchführen, in der alle Risiken und mögliche Interaktionseffekte berücksichtigt werden. Dadurch wird nicht nur das Spektrum aller möglichen Ergebnisse sichtbar, sondern auch die zu den jeweiligen Ergebnissen gehörigen Eintrittswahrscheinlichkeiten.

Welche Bedeutung die Berücksichtigung von Risiken und ihrer Interaktionseffekte hat, sehen Sie am Beispiel DESERTEC: Während das Projekt in einer Betrachtung ohne Risiken für Investoren hoch attraktiv erscheint und auch im Rahmen von Sensitivitätsanalysen nur wenig an Attraktivität verliert, ergibt sich unter simultaner Berücksichtigung aller Risiken und Interaktionseffekte im Rahmen einer simulativen Risikoanalyse eine komplett andere Entscheidungssituation. Das Projekt ist hochgradig unattraktiv und wird in über 99% der Fälle zu einem Verlustgeschäft. Wie das Zusammenwirken der Zutaten in einem Cocktail, führt das Zusammenwirken der Risiken in einem Projekt zu einem oft unterschätzten und hochgradig einflussreichem Effekt (Cocktail-Effekt).

Ausblick

Das Abbilden von Risiken ist allerdings nur ein Aspekt im Risikomanagement von Großprojekten. Bevor Sie die Risiken abbilden können, müssen Sie die möglichen Risiken zunächst systematisch erfassen. Wichtig ist zudem, dass die Projektbeteiligten die Verantwortlichkeiten für bestimmte Risiken klären. Im Projektverlauf spielt es eine große Rolle, mit welchen Maßnahmen Sie die Risiken in Großprojekten absichern. Durch Absicherungsmaßnahmen können Sie den Einfluss von Risiken gegen einen Aufpreis kontrollieren und reduzieren. Alle diese Facetten müssen Sie beim Risikomanagement von Großprojekten berücksichtigen.

Literatur

- Balser, M. / Schneider, J.: Wenn nach einem Vierteljahrhundert die Tür klemmt, Süddeutsche Zeitung vom 22.01.2017, abrufbar unter: <http://www.sueddeutsche.de/wirtschaft/flughafen-berlin-wenn-nach-einem-vierteljahrhundert-die-tuer-klemmt-1.3344249>, letzter Abruf am 05.09.2017
- Flyvbjerg, B.: What You Should Know About Megaprojects and Why: An Overview, in: Project Management Journal, Vol. 45 (2), 2014, S. 6-19
- Flyvbjerg, B.; Bruzelius, N.; Rothengatter, W.: Megaprojects and Risk: Making Decisions in an Uncertain World, Cambridge University Press, Cambridge 2002
- Gausling, P.: *Bewertung und Management von Risiken internationaler Großprojekte. Eine Untersuchung des Einflusses der Partitionierung auf die Risikosituation internationaler Großprojekte am Beispiel der Fallstudie DESERTEC.* Verlag Dr. Kovač, Hamburg 2016
- Gleißner, W.: Die Aggregation von Risiken im Kontext der Unternehmensplanung, in: Zeitschrift für Controlling & Management, Vol. 48 (5), 2004, S. 350-359

- Johnson, N. L.; Kotz, S.: Non-Smooth Sailing or Triangular Distributions Revisited after Some 50 Years, in: The Statistician, Vol. 48 (2), 1999, S. 179-187
- Kanacher, J.; Rademacher, M.; Werner, B.: Risikosimulation als Teil des Projektcontrollings, in: Zeitschrift für Controlling & Management, Vol. 54 (3), 2010, S. 191-198
- Massetti, E.; Ricci, E. C. : An Assessment of the Optimal Timing and Size of Investments in Concentrated Solar Power, in: Energy Economics, Vol. 38 (o. A.), 2013, S. 186-203
- Pollio, G.: International Project Analysis and Financing, Macmillan Press, Houndmills 1999
- Ders.: Realoptionen als Controlling-Instrument: Das Beispiel pharmazeutische Forschung und Entwicklung, Deutscher Universitätsverlag, Wiesbaden 2000
- Reuter, A.: Projektfinanzierung: Anwendungsmöglichkeiten, ÖPP und Infrastrukturfinanzierung, Risikomanagement, Vertragsgestaltung, Kapitalmarkt, bilanzielle Behandlung, 2. Aufl., Schäffer-Poeschel Verlag, Stuttgart 2010
- Trieb, F.; Schillings, C.; Kronshage, S.; Viebahn, P. et. al.: Trans-Mediterranean Interconnection for Concentrating Solar Power (TRANS-CSP): Final Report, Deutsches Zentrum für Luft- und Raumfahrt e. V. (DLR), Stuttgart 2006
- Trieb, F.; Schillings, C.; Pregger, T.; O'Sullivan, M.: Solar Electricity Imports from the Middle East and North Africa to Europe, in: Energy Policy, Vol. 42 (o. A.), 2012, S. 341-353
- Tytko, D.: Grundlagen der Projektfinanzierung, in: Backhaus, K.; Werthschulte, H. (Hrsg.): Projektfinanzierung: Wirtschaftliche und rechtliche Aspekte einer Finanzierungsmethode für Großprojekte, 2. Aufl., Schäffer-Poeschel Verlag, Stuttgart, 2003, S. 11-36
- Ummel, K.; Wheeler, D.: Desert Power: The Economics of Solar Thermal Electricity for Europe, North Africa, and the Middle East, Working Paper, Center for Global Development, 2008
- Werthschulte, H.: Kreditrisikomessung bei Projektfinanzierungen durch Risikosimulation, Deutscher Universitätsverlag, Wiesbaden 2005
- Williges, K.; Lilliestam, J.; Patt, A.: Making Concentrated Solar Power Competitive with Coal: The Costs of a European Feed-in Tariff, in: Energy Policy, Vol. 38 (6), 2010, S. 3089-3097
- Zickfeld, F.; Wieland, A.; Bartolot, J. et. al.: Desert Power: Getting Started: The Manual for Renewable Electricity in MENA, Full Report, Dii GmbH, München 2013

Wenn man vor lauter Bäumen den Wald nicht mehr sieht

Die 4 Os zur Risikoidentifikation in Großprojekten



Dr. Philipp Gausling

Projektmanager und Experte
für das Risikomanagement
von Großprojekten

Management Summary

- Risikomanager von Großprojekten übersehen oft einzelne Risiken. Gründe dafür sind die individuelle Ausgestaltung und Komplexität von Großprojekten, die zu einer Vielzahl und zum Teil sehr projekt-spezifischen Risiken führen.
- In 9 von 10 Großprojekten kommt es zu wesentlichen Kostenüberschreitungen und Verzögerungen aufgrund falsch eingeschätzter oder übersehener Risiken.
- Es fehlt an Ansätzen zur systematischen und ganzheitlichen Erfassung von Risiken. Diese sind jedoch elementar, um den Einfluss von Risiken auf das Projekt richtig einzuschätzen und ggf. gezielte Maßnahmen zur Risikoprävention und -absicherung ergreifen zu können.
- Die 4 Os zur Risikoidentifikation stellen ein Konzept zur systematischen und ganzheitlichen Erfassung von Risiken dar. Die 4 Os stehen für operative, organisatorische, ökonomische und ortsabhängige Risiken.
- Der Beitrag fasst die bereits bestehenden Risikokataloge in einem universalen Katalog zusammen, liefert klare Definitionen für die einzelnen Risikoarten und veranschaulicht diese anhand konkreter Beispiele aus realen Großprojekten. Dadurch fördert er ein einheitliches und eindeutiges Verständnis möglicher Risikoarten in Großprojekten.

Dem Risikomanager fällt es schwer, vor lauter Bäumen den Wald noch zu sehen

In 9 von 10 Großprojekten kommt es zu Planungsabweichungen im Hinblick auf die Projektkosten und -dauer aufgrund falsch eingeschätzter oder übersehener Risiken (vgl. Flyvbjerg, 2014). Denn aufgrund ihrer Komplexität sind Großprojekte mit einer Vielzahl von Risiken behaftet. Dabei gleicht kein Projekt dem anderen: Da Großprojekte äußerst unterschiedlich gestaltet sein können, treten zum Teil sehr projektspezifische Risiken auf. Aufgrund dieser Tatsache und der hohen Anzahl möglicher Risiken passiert es oft, dass Risikomanager einzelne Risiken übersehen. Dies kann schwerwiegende Folgen haben, wie z.B. beim Berliner Flughafen (BER).

Beim BER wurde lange Zeit ein technisches Risiko übersehen, sodass der Flughafen die erforderlichen Brandschutzbestimmungen nicht erfüllen konnte. Ursprünglich sollten im Falle eines Brands mobile Rauchschürzen zwischen Terminal und Tiefbahnhof die Ausbreitung von Qualm verhindern. Da dies nicht funktionierte, werden stattdessen Glaswände errichtet, die eine neue Baugenehmigung voraussetzen. Neben langen Verzögerungen in der Fertigstellung und den teuren Umbauten müssen zudem teure Computersimulationen bezüglich der Entrauchung wiederholt werden (vgl. hier und in diesem Abschnitt Metzner, 2017a). Aufgrund einer Verkettung derartiger Vorfälle hat sich die geplante Eröffnung des Flughafens mittlerweile von 2011 auf 2020 verschoben (vgl. Metzner, 2017b).

Dieses Beispiel zeigt, wie wichtig es ist, alle Risiken für ein Großprojekt zu erfassen. Fehler wie beim Berliner Flughafen gilt es bei der Planung zu vermeiden, damit zum einen der Einfluss der Risiken auf das Projekt besser eingeschätzt werden kann und zum anderen gezielte Maßnahmen gegen diese Risiken ergriffen werden können.

Im vorliegenden Beitrag stelle ich mit den 4 Os zur Risikoidentifikation von Großprojekten ein Konzept vor, mit dem Sie systematisch eine vollständige Übersicht über mögliche Risiken in Großprojekten erlangen. Dieser hat sich bereits bei Risikoanalysen von Großprojekten wie dem DESERTEC-Projekt und der Nord-Stream Pipeline (in leicht abgewandelter Form) bewährt (vgl. Gausling (2016), DIN SPEC 91331:2015-11). In diesem Zusammenhang definiere ich auch mögliche Risikoarten, veranschauliche diese anhand von konkreten Projektbeispielen und arbeite die Einsatzmöglichkeiten des Risikokatalogs im Prozess der Risikoidentifikation heraus.

Dieser Beitrag richtet sich an alle Initiatoren und Planer von Großprojekten wie staatliche Institutionen, Unternehmen, Projektleiter oder Projektgesellschaften, sowie an alle Risikomanager und weitere am Risikomanagement von Großprojekten Interessierte. Ich möchte Sie für die Vielfalt unterschiedlicher Risiken in Großprojekten sensibilisieren und einen selbst entwickelten Risikokatalog präsentieren, der eine systematische und ganzheitliche Erfassung von Risiken in Großprojekten ermöglicht.

Was sind eigentlich Risiken und wie werden sie kategorisiert?

In der Fachliteratur wird Risiko als die "negative Abweichung vom Erwartungswert einer Zielgröße [...], die aus einer Fehlentscheidung aufgrund unvollkommener Informationen im Entscheidungszeitpunkt resultiert" (Gausling, 2016) aufgefasst. Risiko sollte jedoch als eine mehrdimensionale Größe verstanden werden: Gerade in einem Großprojekt kann eine Vielzahl unterschiedlicher Risiken eintreten, die sich zudem gegenseitig bedingen (siehe dazu den Fachbeitrag "[Abbildung von Risiken in Großprojekten oder was Risiken und Cocktails gemeinsam haben](#)"). Damit Sie einen systematischen Überblick über die Gesamtheit der relevanten Risiken bekommen, sollten Sie diese kategorisieren.

Die Kategorisierung stellt den ersten Schritt bei der Risikoidentifikation dar, die als Frühwarnsystem zum Erkennen von Projektrisiken etablierter Bestandteil eines projektweiten Risikomanagementsystems ist (siehe dazu den Methodensteckbrief "[Risikokatalog](#)"). Da die Kategorisierung wesentlicher Bestandteil der Risikoidentifikation ist und sich somit unmittelbar und wesentlich auf den weiteren Prozess des Risikomanagements auswirkt, kommt der Kategorisierung im Folgenden besondere Bedeutung zu.

Zur Kategorisierung haben sich in der Praxis folgende drei Kriterien etabliert:

1. die **Ursache** des Risikos

2. die **Projektphase**, in der das Risiko auftritt
3. der **Risikoverantwortliche**, der die Verantwortung für das Risiko trägt

Kategorisieren nach Risikoursache

Um eine überschneidungsfreie Kategorisierung zu erreichen, empfehle ich Ihnen, Risiken zunächst nach ihrer Ursache zu kategorisieren. Denn weder eine Kategorisierung nach Projektphasen noch eine Zuordnung zu bestimmten Risikoverantwortlichen führen zu überschneidungsfreien Kategorien.

Zum einen kann es sein, dass Risiken phasenübergreifenden Einfluss haben. Ein politisches Risiko kann beispielsweise sowohl in der Planungs-, der Bau- als auch der Betriebsphase des Projekts eintreten. Zum anderen kann es sein, dass Risiken nicht sinnvoll oder gleich mehreren Beteiligten zugeordnet werden können. So kann das Finanzierungsrisiko sowohl Investoren, Banken als auch subventionierenden Staaten zugeschrieben werden.

Ein Risikokatalog für Großprojekte

Sowohl in der Literatur als auch in der Praxis besteht bereits eine Vielzahl verschiedener Risikokataloge (vgl. z.B. Böttcher/Blattner, 2013, DIN SPEC 91331:2015-11, Pollio, 1999, Tinsley, 2000, Yescombe, 2014). Diese gehen allerdings zum Teil von unterschiedlichen Risikokategorien und Definitionen der Risikoarten aus. 15 der in der Fachliteratur gängigsten Risikokataloge für Großprojekte habe ich daher zu einem einzelnen Risikokatalog zusammengefasst, der einen umfassenden und systematischen Überblick über Risikoarten in Großprojekten gibt, die einzelnen Risikoarten klar definiert und durch Beispiele veranschaulicht.

Anzahl der Oberkategorien

Auf der obersten Ebene unterscheide ich, wie in Bild 1 dargestellt, zwischen operativen, organisatorischen, ökonomischen und ortsabhängigen Risiken. Während die operativen und organisatorischen Risiken vorwiegend projektinternen Ursprungs sind, beruhen die ökonomischen und ortsabhängigen Risiken auf projektexternen Einflüssen. Da alle diese Risikofelder mit dem Buchstaben O (bzw. Ö) beginnen, bezeichne ich meinen Kategorisierungsansatz als "die 4 Os zur Risikoidentifikation in Großprojekten".



Bild 1: Die 4 Os zur Risikoidentifikation in Großprojekten

Anzahl der Strukturebenen

Diese vier Kategorien lassen sich jeweils in weitere Unter- und Unterunterkategorien unterteilen. Um das Risiko differenziert betrachten zu können, aber immer noch eine gute Übersichtlichkeit zu gewährleisten, beschränkt sich der Katalog auf drei Ebenen. Eine zunächst grobe Risikoeinteilung ist sinnvoll, um den Überblick über die Vielzahl der Risiken in einem Projekt zu behalten.

In der Detailplanung eines Projekts ist es jedoch in der Regel hilfreich, projekt- und risikospezifisch weitere Unterteilungen vorzunehmen. Ist ein Projekt beispielsweise von besonders vielen Risiken einer Risikokategorie betroffen, kann eine weitere und spezifischere Unterteilung dieser Risikokategorie nützlich sein, um differenzierte Maßnahmen gegen die einzelnen Risiken zu ergreifen.

Werden für ein Projekt beispielsweise besonders vielfältige und bedeutsame politische Risiken [Unterteilung: Ortsabhängiges Risiko (Ebene 1) - Länderrisiko (Ebene 2) - Politisches Risiko (Ebene 3)] identifiziert, könnte eine weitere Unterteilung der politischen Risiken in das Enteignungsrisiko, das Eingriffsrisiko, das Risiko politischer Instabilität und das Risiko politisch motivierter Kriege und Revolutionen sinnvoll sein (Ebene 4), um gezielte Maßnahmen zu erörtern. Der jeweilige Detaillierungsgrad der einzelnen Risikokategorien sollte daher je nach Risikosituation des Projekts individuell bestimmt werden.

Im folgenden Abschnitt stelle ich die 4 Os zur Risikoidentifikation mitsamt den dazugehörigen Unterkategorien näher vor und erläutere sie an Beispielen.

Die 4 Os zur Risikoidentifikation in Großprojekten

1. Operative Risiken

Die operativen Risiken umfassen alle Risiken, die den Ablauf der Projektaktivitäten betreffen. Dazu gehören das Zulieferisiko, das Fertigstellungsrisiko, das Betriebsrisiko, das Managementrisiko und das Technikrisiko (siehe Bild 2).

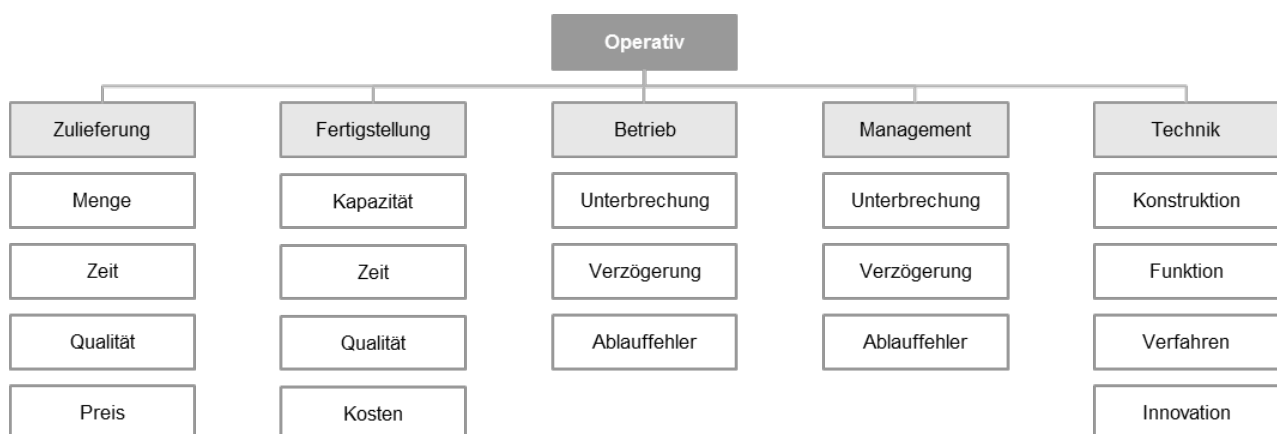


Bild 2: Überblick über operative Risiken

Zuliefererrisiko

Das Zuliefererrisiko beschreibt das Risiko, dass die Zulieferung von Roh-, Hilfs- und Betriebsstoffen nicht in der benötigten Menge, in der geplanten Zeit, in benötigter Qualität oder zu den prognostizierten Preisen erfolgt.

Beispiel

Nord Stream Pipeline

Gaspipeline
Bauzeit: 2005-2013
Kosten: 7,4 Mrd. €

Bei der Nord Stream Pipeline mussten für den Bau der Leitungen 90 Millionen Tonnen Eisen und Beschichtungsmaterial über weite Distanzen in verschiedene Länder transportiert werden. Es bestand das Risiko, dass der Logistikplan nicht eingehalten wird und die Lieferungen nicht im benötigten Umfang und zur geplanten Zeit am Zielort ankommen (vgl. Nord Stream AG, 2013; DIN SPEC 91331:2015-11, 2015).

Fertigstellungsrisiko

Das Fertigstellungsrisiko beschreibt das Risiko, dass die Fertigstellung gar nicht, verzögert, zu geringeren Kapazitäten oder zu höheren Kosten erfolgt.

Beispiel

Flughafen BER

Flughafen
Bau: 2006-2020 (geplant)
Kosten: 7,3 Mrd. €

Beim Flughafen Berlin Brandenburg musste der Eröffnungstermin aufgrund vieler Planungsfehler, Fehleinschätzungen und Baumängel mehrmals nach hinten verschoben werden. Statt wie ursprünglich geplant 2011 wurde als neuer vorläufiger Eröffnungstermin zuletzt das Jahr 2020 genannt (vgl. Spiegel, 2018).

Neben den deutlich höheren Kosten (Anstieg von ursprünglich 2,1 Mrd. € auf 7,3 Mrd. €) muss als Konsequenz der späteren Fertigstellung auch ein Verlust von Einnahmen durch den ausbleibenden Betrieb des Flughafens hingenommen werden.

Betriebsrisiko

Das Betriebsrisiko beschreibt das Risiko, dass es zu Unterbrechungen, Verzögerungen oder fehlerhaften Abläufen im Betrieb kommt.

Beispiel

Nord Stream Pipeline

Gaspipeline
Bau: 2005-2013
Kosten: 7,4 Mrd. €

Beim Betrieb der Nord Stream Pipeline kann es zu Abweichungen des Drucks, der Temperaturen, der Fließgeschwindigkeit und der Eigenschaften des Gases kommen. Es besteht daher die Gefahr, dass eine termingerechte Beförderung des Gases in benötigter Menge und Qualität ausbleibt (vgl. Nord Stream AG, 2013; DIN SPEC 91331:2015-11, 2015).

Managementrisiko

Das Managementrisiko beschreibt das Risiko, dass sich Fehler auf Führungsebene auf den Projekterfolg auswirken. Wie beim Betriebsrisiko kann es dadurch zu Unterbrechungen, Verzögerungen und fehlerhaften Abläufen im Projekt kommen.

Beispiele

Flughafen BER

Flughafen

Beim Flughafen Berlin-Brandenburg führten Fehler des Managements zu fehlerhaften Abläufen und Verzögerungen. Die Flughafengesellschaft Berlin-Brandenburg (FBB), deren Expertise im Betrieb, aber nicht im Bau von Flughäfen liegt, wurde mit dem Bau des Flughafens betraut.

Bau: 2006-2020 (geplant) Kosten: 7,3 Mrd. €	Statt mit Fachexperten wurde der Aufsichtsrat vorwiegend mit Politikern besetzt. Auf einen Generalunternehmer wurde verzichtet und die Projekte auf viele Unterauftragnehmer verteilt. Die führte unter dem Zeitdruck des Eröffnungstermins zu einer Fehlerspirale aus simultanen Planen und Bauen, ständigen Planänderungen und großen Koordinationsschwierigkeiten (vgl. Fiedler/Wendler, 2015).
Elbphilharmonie Konzerthaus Bau: 2007-2016 Kosten: 866 Mio. €	Das Missmanagement bei der Elbphilharmonie wurde bereits vor Baubeginn deutlich. Die Stadt verteilte den Bauauftrag, bevor sie das Projektvorhaben überhaupt vollständig definiert hatte. Im Nachgang gab es viele Planungsänderungen und hohe Nachforderungen. Der Bürgermeister blieb dabei lange Zeit untätig. Eine effektive Kostenkontrolle blieb aus (vgl. Ritter/Müssgens, 2013).

Technikrisiko

Das technische Risiko umfasst alle Risiken, die einen technischen Ursprung haben. Dazu gehören vier Unter-
risiken: (1) Das Konstruktionsrisiko beschreibt die Gefahr, dass es bei der Konstruktion technische Schwierig-
keiten gibt. (2) Das Funktionsrisiko liegt vor, wenn das Projekt aufgrund fehlerhafter Technik nicht wie ge-
plant verläuft. (3) Das Verfahrensrisiko zeigt sich, wenn es im Betrieb zu verfahrenstechnischen
Unterbrechungen oder Verzögerungen kommt. (4) Das Innovationsrisiko besteht, wenn innovative technolo-
gische Neuerungen das Projekt unwirtschaftlich und nicht wettbewerbsfähig machen.

Beispiele	
Flughafen BER Flughafen Bau: 2006-2020 (geplant) Kosten: 7,3 Mrd. €	Beim Berliner Flughafen gab es technische Probleme, da die ursprüngliche Konstruktion zum Brandschutz nicht entsprechend der Brandschutzbestimmungen funktionierte. Stattdessen muss nun eine neue Glaswandkonstruktion errichtet werden, für die neue Baugenehmigungen und Tests durch teure Computersimulationen erforderlich werden (vgl. Metzner, 2017a).
Biocéánico Bahnlinie Bau: in Planung Kosten: ca. 13 Mrd. €	Beim Biocéánico sollen die Anden mit einer Eisenbahnschiene durchquert werden. Da ein Großteil der Strecke noch nicht erschlossen ist und der Bau mehrere Tunnel mit bis zu 52 km Länge beinhaltet, steht das Projekt vor großen technologischen Herausforderungen (vgl. Gausling, 2017a, " Der Ozean-Express: Zukunftsvision oder Größenwahn? ").
Stuttgart 21 Bahnanlagen Bau: 2010-2024 (geplant) Kosten: ca. 7,6 Mrd. €	Im Rahmen von Stuttgart 21 versucht die Bahn unter anderem einen Kopfbahnhof durch einen Durchgangsbahnhof zu ersetzen. In diesem Zuge muss die Bahn Tunnel von 60 km Länge durch die umliegenden Berge bauen. Die spezielle Geografie und Geologie stellt das Projekt dabei vor technologische Herausforderungen (vgl. Spiegel, 2017).

2. Organisatorische Risiken

Zu den organisatorischen Risiken gehören alle Risiken, die den Aufbau der Projektorganisation betreffen. Dazu gehören das Vertragsrisiko, das Abandonrisiko und das Internationalitätsrisiko (siehe Bild 3).

Vertragsrisiko

Das Vertragsrisiko beschreibt das Risiko, dass es zu einer Nicht-Einigung zwischen den Projektparteien aufgrund von Zielkonflikten, zur Nicht-Erfüllung des Vertrags oder aufgrund rechtlicher Restriktionen zur Nicht-Durchsetzbarkeit des Vertrags kommt.

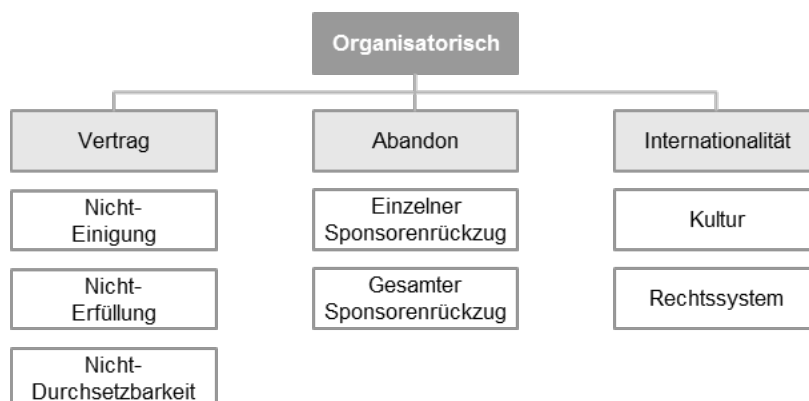


Bild 3: Überblick über organisatorische Risiken

Beispiele

Nord Stream Pipeline

Gaspipeline
Bau: 2005-2013
Kosten: 7,4 Mrd. €

Bei den Verhandlungen mit Estland gab es Probleme bei der Vertragsgestaltung. Der Antrag, dass die Nord Stream Pipeline durch estländische Gewässer verlaufen darf, wurde abgelehnt. Schließlich musste die Pipeline durch finnische Gewässer geführt werden, was einen erheblichen Umweg bedeutete (vgl. Nord Stream AG, 2013; DIN SPEC 91331:2015-11, 2015).

Elbphilharmonie

Konzerthaus
Bau: 2007-2016
Kosten: 866 Mio. €

Bei der Elbphilharmonie herrschten zwischen dem Generalunternehmer Hochtief, den Architekten und der Stadt aufgrund der komplizierten Vertragsstruktur immer wieder Meinungsverschiedenheiten, Durcheinander und Blockierungen. Die Parteien gaben sich gegenseitig die Schuld für Verzögerungen und Mängel am Bau. Anders als bei Großprojekten üblich, gab es keinen direkten Kommunikationsweg zwischen dem Baukonzern und den Planern. Stattdessen fungierte die Realisierungsgesellschaft als Mittler zwischen Vertragspartnern, den Architekten und dem Bauunternehmen und war mit der Informationsflut überfordert (vgl. Ritter/Müssgens, 2013).

Abandonrisiko

Das Abandonrisiko beschreibt die Gefahr, dass entweder einzelne oder alle Sponsoren das Projekt vorzeitig verlassen. Verlassen nur einzelne Sponsoren das Projekt, kann ggf. nach alternativen Investoren gesucht werden. Ziehen sich jedoch alle Sponsoren vorzeitig aus dem Projekt zurück, bedeutet dies den sicheren Projektabbruch.

Beispiel

DESERTEC

Energieinfrastrukturprojekt
Bau: 2010/2050 (Abbruch)
Kosten: ca. 180 Mrd. €

2013 kam es im Desertec-Projekt zu Meinungsverschiedenheiten unter den Parteien im Hinblick auf die Solarstromexporte von Afrika nach Europa. Einige Gesellschafter der bis auf 21 Shareholder und 35 assoziierten Partner angewachsenen Desertec Industrial Initiative (Dii GmbH) zur Umsetzung des Desertec Projekts in der EUMENA-Region verließen daraufhin das Projekt (vgl. DESERTEC Foundation, 2015; Dii GmbH, 2015).

Auf einer Gesellschafterversammlung am 13. Oktober 2014 in Rom beschlossen die 17 noch verbliebenen Gesellschafter schließlich, die Dii GmbH nur fünf Jahre nach ihrer Gründung in ihrer derartigen Form als Planungsgesellschaft aufzulösen und in ein stark verkleinertes Beratungsunternehmen zu überführen. Von den zuletzt noch 20 Gesellschaftern der Dii GmbH blei-

ben lediglich der deutsche Energieversorger RWE, die saudi-arabische Energiefirma ACWA Power und der chinesische Netzbetreiber State Grid (SGCC) (vgl. Basler, 2014; Frankfurter Allgemeine Zeitung, 2014).

Internationalität

Das Internationalitätsrisiko beschreibt die Gefahr, die aus der Internationalität des Projekts resultiert. Es kann zu Unterschieden im Hinblick auf die Kultur oder das Rechtssystem kommen. Kulturelle Unterschiede können beispielsweise aufgrund ungleicher Wertsysteme, Mentalitäten oder Sprachen der Projektbeteiligten bestehen und zu Konflikten, Missverständnissen und Verständigungsschwierigkeiten im Projekt führen. Unterschiedliche Rechtssysteme können beispielsweise dazu führen, dass sich Rechtsnormen zweier Länder widersprechen und zu Streitigkeiten zwischen internationalen Vertragspartnern führen.

Beispiel

DESERTEC

Energieinfrastrukturprojekt
Bau: 2010-2050 (Abbruch)
Kosten: ca. 180 Mrd. €

Beim DESERTEC-Projekt mussten viele Personen mit unterschiedlichen Nationalitäten und Wertvorstellungen über Ländergrenzen hinweg zusammenarbeiten. Aufgrund der vielen unterschiedlichen Kulturen und Wertesysteme im Projekt bestand die Gefahr von Konflikten und Abstimmungsschwierigkeiten in der Zusammenarbeit (vgl. Gausling, 2016).

3. Ökonomische Risiken

Zu den ökonomischen Risiken gehören alle Risiken, die einen wirtschaftlichen Ursprung haben. Diese können in das Finanzierungsrisiko, das Kreditrisiko, das Marktrisiko und das Ressourcenrisiko unterteilt werden, wie Bild 4 zeigt.

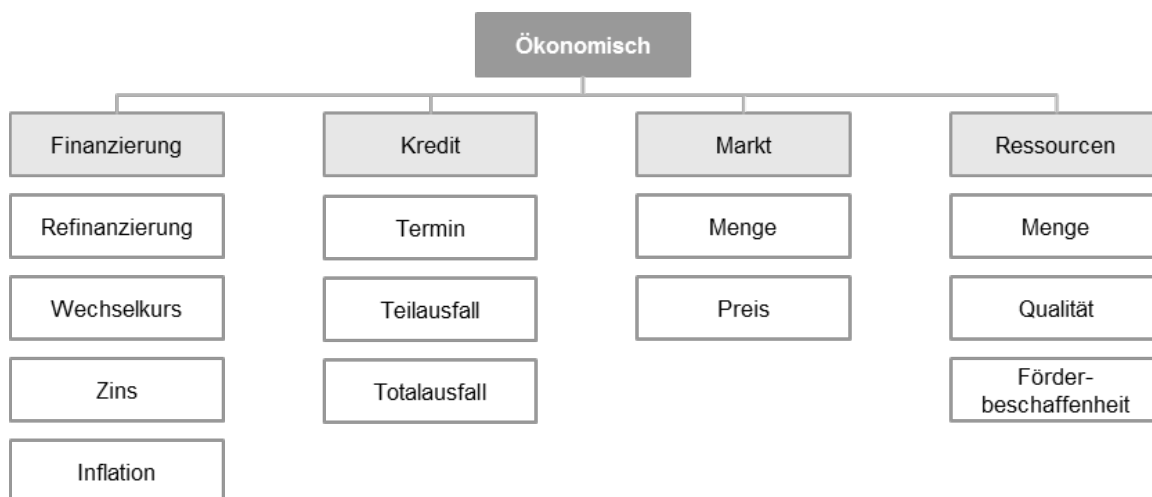


Bild 4: Überblick über ökonomische Risiken

Finanzierungsrisiko

Das Finanzierungsrisiko umfasst alle Risiken, die die Finanzierung des Projekts betreffen. Dazu gehören das Refinanzierungsrisiko, das Wechselkursrisiko, das Zinsrisiko und das Inflationsrisiko. Das Refinanzierungsrisiko beschreibt die Gefahr, dass die Refinanzierung durch die Fremdkapitalgeber nicht im gewünschten Umfang oder zu den erwarteten Konditionen erfolgen kann.

Das Wechselkursrisiko liegt vor, wenn es zu zeitlichen oder betragsmäßigen Währungsunterschieden auf Einzahlungs- und Auszahlungsseite kommt, die eine Überführung einer Währung in eine andere zu möglichen Wechselkursverlusten erforderlich machen. Das Zinsrisiko besteht, wenn der Zinssatz während der Kreditlaufzeit nicht fixiert ist und schwankt. Das Inflationsrisiko beschreibt das Risiko, dass Änderungen des Preisniveaus auftreten.

Beispiel

Nord Stream Pipeline

Gaspipeline
Bau: 2005-2013
Kosten: 7,4 Mrd. €

Die Finanzkrise in den Jahren 2008 und 2009 erhöhte bei vielen Investoren und Auftragnehmern das Risiko der Insolvenz und des vorzeitigen Ausstiegs aus dem Projekt (vgl. Nord Stream AG, 2013; DIN SPEC 91331:2015-11, 2015).

Kreditrisiko

Das Kreditrisiko beschreibt die Gefahr, dass ein Fremdkapitalgeber die vergebenen Kredite nicht zum festgelegten Termin, nur zum Teil oder überhaupt nicht wiederbekommt. Bei einem hohen Kreditrisiko müssen für Kredite häufig höhere Zinsen gezahlt werden. Zugleich wird es schwieriger, weitere Kredite für das Projekt zu bekommen.

Beispiel

Nord Stream Pipeline

Gaspipeline
Bau: 2005-2013
Kosten: 7,4 Mrd. €

Durch die Finanzkrise in 2008 und 2009 bestand die Gefahr, dass es zu Liquiditätsengpässen kommt und Kredite nicht zurückgezahlt werden können (vgl. Nord Stream AG, 2013; DIN SPEC 91331:2015-11, 2015).

Marktrisiko

Das Marktrisiko beschreibt das Risiko, dass am Markt die geplante Absatzmenge oder der geplante Preis nicht erzielt werden kann, sodass es zu Umsatzverlusten kommt.

Beispiel

DESERTEC

Energieinfrastrukturprojekt
Bau: 2010-2050 (Abbruch)
Kosten: ca. 180 Mrd. €

Gerade im Energiemarkt gibt es viele technologische Neuerungen und Konkurrenzanbieter, sodass man unter Umständen die Preise, mit denen man heute kalkuliert, in Zukunft wesentlich verfehlt. Für eine sichere Prognose der Einzahlungen muss zudem die Energieabnahme der ersten Jahre im Projektzeitraum sichergestellt werden. Dies ist aber aufgrund der dynamischen Entwicklungen am Energiemarkt und des langfristigen Projektzeitraums nur schwer bis gar nicht zu gewährleisten.

Ressourcenrisiko

Das Ressourcenrisiko beschreibt das Risiko, dass benötigte Ressourcen nicht in erforderlicher Menge, Qualität oder Förderbeschaffenheit verfügbar sind.

Beispiel	
Nord Stream Pipeline Gaspipeline Bau: 2005-2013 Kosten: 7,4 Mrd. €	Die Nord Stream Pipeline konkurrierte damals stark mit anderen Offshore-Projekten von ebenfalls bekannten Energieunternehmen um Ressourcen wie Stahl. Es war lange Zeit unsicher, ob genügend Ressourcen beschafft werden können, um das Projekt fristgerecht fertigzustellen (vgl. Nord Stream AG, 2013; DIN SPEC 91331:2015-11, 2015).

4. Ortsabhängige Risiken

Zu den ortsabhängigen Risiken gehören alle Risiken, die sehr stark vom Projektstandort abhängen. Dazu gehören das Force-Majeure-Risiko, das Umweltrisiko und das Länderrisiko (siehe Bild 5).

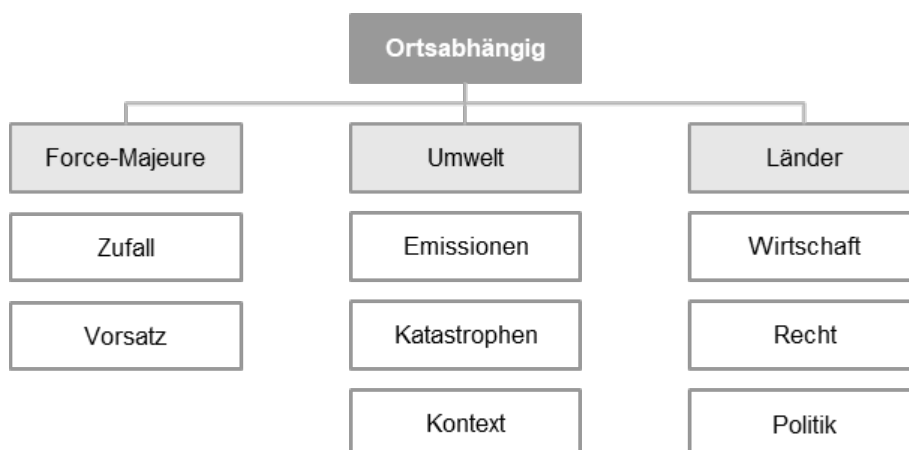


Bild 5: Überblick über ortsabhängige Risiken

Force-Majeure-Risiko

Das Force-Majeure-Risiko beschreibt alle Risiken höherer Gewalt. Diese können zum einen durch den Zufall hervorgerufen werden wie bei Naturereignissen (z.B. Erdbeben, Unwetter oder Epidemien). Zum anderen können sie auch vorsätzlich veranlasst werden (z.B. Streik, Terrorismus).

Beispiel	
Biocéánico Bahnlinie Bau: in Planung Kosten: ca. 13 Mrd. €	In den Anden sind Naturkatastrophen wie Erdbeben, Sturzfluten, Erdbeben oder vulkanische Aktivitäten keine Seltenheit. Vor diesen Gefahren müssen die Tunnel durch die Anden abgesichert sein (vgl. Gausling, 2017a).

Umweltrisiko

Das Umweltrisiko beschreibt das Risiko, dass das Projekt die Umwelt belastet. Dies kann durch Emissionen (z.B. von CO₂), Umweltkatastrophen (z.B. eine brennende Ölquelle) und den Kontext (z.B. Aktivitäten von Umweltaktivisten) hervorgerufen werden. Neben Fragen der Moral können solche Verfehlungen Projekte durch negative Publicity und juristische Sanktionen belasten, wie Strafzahlungen und Freiheitsentzug für Projektverantwortliche.

Beispiel

Suezkanal

Schifffahrtskanal
Bau: 1859-1869
Kosten: 19 Mio. Pfund

Durch den vor ca. 150 Jahren gebauten Suezkanal nahmen die Ökosysteme im Mittelmeerraum erheblichen Schaden. Über 400 fremde Spezies, darunter auch aggressive Arten, fielen ins Mittelmeer ein und konnten sich dort schnell ausbreiten, da natürliche Feinde wie Raubtiere oder Parasiten fehlten. Ein Beispiel ist die hochgiftige Quallenart *Rhopilema nomadica*, die erstmals 1970 im Mittelmeer gesichtet wurde und durch ihre rasante Ausbreitung seither den Fischfang sowie den Tourismus in bestimmten Mittelmeergebieten erschwert (vgl. Conrad, 2015; Ägypten Magazin, 2018).

Länderrisiko

Das Länderrisiko umfasst alle Risiken, die mit dem Land, in dem das Projekt realisiert wird, im Zusammenhang stehen. Diese können wirtschaftlichen, rechtlichen oder politischen Ursprungs sein. Unter die wirtschaftlichen Risiken fallen das Verbot der Konvertierung der Landeswährung in eine Fremdwährung, das Verbot des Geld-transfers in ein anderes Land oder ein generelles Zahlungsverbot. Unter den rechtlichen Risiken werden hingegen Risiken im Zusammenhang mit dem Rechtssystem eines Landes verstanden. Diese bestehen z.B. in der Gefahr von Gesetzesänderungen oder im Widerruf von Genehmigungen. Zu den politischen Risiken gehören schließlich alle Risiken, die unter die Hoheitsgewalt des Staates fallen, wie z.B. die Enteignung von Vermögen oder der Eingriff in Personalentscheidungen.

Beispiel

Biocéánico

Bahnlinie
Bau: in Planung
Kosten: ca. 13 Mrd. €

Mit Bolivien, Brasilien und Peru sind drei Länder beim Biocéánico Projekt involviert, die politisch und wirtschaftlich schwierige Rahmenbedingungen bieten. Die Staaten verfügen über hohe bürokratische Hürden – z.B. bezogen auf Genehmigungen –, was das gesamte Projekt verzögern kann. Zudem nehmen Behörden dort oft Einfluss auf unternehmerische Tätigkeiten. Das politische Umfeld ist somit sehr schwierig. Fachkräfte dürften in diesen Ländern ebenfalls schwer zu finden sein. Die Rechtssicherheit ist außerdem deutlich geringer als z.B. in Europa. (vgl. Gausling, 2017a).

Einsatz der 4 Os im Prozess der Risikoidentifikation

Die im vorangegangenen Kapitel vorgestellten 4 Os sind ein wertvolles Instrument bei der Identifikation von Risiken in Großprojekten, da sie bei einer systematischen und vollständigen Erfassung aller Risiken helfen. Die vollständige Identifikation aller Risiken bildet den Grundstein für eine erfolgreiche Projektplanung und einen reibungslosen Projektverlauf.

2 Phasen mit verschiedenen Teams

Um bei der Risikoerfassung möglichst sorgsam vorzugehen, sollte der Prozess der Risikoidentifikation in zwei Phasen erfolgen, wie in Bild 6 dargestellt. In der ersten Phase sollte ein Kernteam die Risikoschwerpunkte im Projekt bestimmen.

In der zweiten Phase sollten Fachteams die Risiken innerhalb der Schwerpunkte im Detail herausarbeiten. Sowohl das Kernteam als auch die Fachteams können sich für eine systematische und möglichst vollständige Erfassung der Risiken an den 4 Os zur Risikoidentifikation als Risikokatalog orientieren.



Bild 6: Einsatz der 4 Os im Prozess der Risikoidentifikation

1. Phase: Kernteam setzt Schwerpunkte

Im Detail gestaltet sich der Prozess der Risikoidentifikation wie folgt: Zu Beginn der ersten Phase sollten Sie als Projektleiter ein Kernteam definieren, das für das Projekt verantwortlich ist. Dies kann je nach Größe und Komplexität des Projekts unterschiedlich groß sein, sollte aber aus Gründen der Effizienz möglichst klein gehalten werden. Basierend auf empirischen Untersuchungen von Hoegle (2005) gilt eine Teamgröße von drei bis sechs Mitgliedern dabei als optimal.

Für das Kernteam ist es zunächst wichtig, ein gemeinsames und tiefes Projektverständnis zu schaffen. Dazu müssen alle relevanten Informationen gesammelt werden, die Aufschluss über das Projekt und seine spezifischen Besonderheiten geben. Das können projektspezifische Dokumente wie die Projektbeschreibung, der Projektauftrag, der Projektstrukturplan, der Businessplan oder Kosten- und Ablaufpläne sein (vgl. Niklas, 2017).

Auch bereits durchgeführte Analysen und Gutachten gehören dazu sowie Erfahrungen aus bereits abgewickelten und vergleichbaren Projekten. Diese können unternehmensinternen Projektdatenbanken entnommen werden.

Auch in externen Internetquellen lassen sich oft relevante Informationen zu vergleichbaren Projekten finden (siehe dazu den Fachbeitrag "[Wie finden Sie die relevanten Informationen für Ihr Projekt?](#)"). Um das Wissen zusammenzutragen und einen gemeinschaftlichen Zugriff zu erlauben, bietet sich z.B. die Einrichtung eines Wikis bzw. einer webbasierten Dokumentationsplattform an.

Auf Grundlage der gesammelten Informationen kann das Kernteam eine erste Analyse zur Identifikation von Risiken durchführen. Hier kommt zum ersten Mal der vorgestellte Risikokatalog bzw. die 4 Os zur Risikoidentifikation

zum Einsatz. Um ein systematisches Vorgehen zu gewährleisten und keine Risikobereiche zu übersehen, sollten die 4 Os zur Risikoidentifikation und deren Unterkategorien im Kernteam der Reihe nach diskutiert und analysiert werden. Zur Feststellung der Risiken in den einzelnen Kategorien eignen sich verschiedene Methoden wie z.B. das **Brainstorming**, das **Mind Mapping** oder auch das **Ishikawa-Diagramm** (vgl. Niklas, 2017).

2. Phase: Deep Dive der Fachteams

Nachdem das Kernteam die Risikoschwerpunkte im Projekt identifiziert hat, ist es in der zweiten Phase sinnvoll, auf Grundlage der Risikoschwerpunkte Fachteams zu spezifizieren. Gerade in Kategorien, in denen viele Risiken vermutet werden, ist es wichtig, Fachexperten einzusetzen, die Erfahrung, einen geschulten Blick und ein feines Gespür für mögliche Risiken mitbringen.

Identifiziert das Kernteam des Großprojekts beispielsweise die Beschaffung von Materialien als Risikoschwerpunkt, könnten beispielsweise gezielt Einkäufer und Logistiker in einem Fachteam eingesetzt werden, die häufig mit der Beschaffung von Materialien und damit verbundenen Risiken zu tun haben.

Fehlt es intern an Expertise, können Sie gegebenenfalls auch Externe wie beispielsweise fachnahe Professoren, erfahrene Berater oder unabhängige Experten aus der Praxis mit in das Fachteam einbinden. Dieses spezifische Fachteam beschäftigt sich dann ausschließlich mit der Ausarbeitung der Risiken seiner Risikoschwerpunktkategorie.

Auch die Fachteams benötigen zunächst ein tieferes Projektverständnis. Dazu sollten sie von mindestens einem Vertreter aus dem Kernteam eine Einweisung in das Projekt bekommen und beispielsweise über das eingerichtete Projekt-Wiki Zugriff auf alle relevanten Informationen im Projekt erhalten.

Unter Aufsicht eines Verantwortlichen aus dem Kernteam kann nun eine zweite Phase zur Identifikation von Risiken eingeleitet werden, die in den einzelnen Fachteams stattfindet. Der Einsatz verschiedener Fachteams erlaubt einen sogenannten Deep Dive in die 4 Os zur Risikoidentifikation.

In dieser Phase ist es aufgrund des spezifischen Know-hows der Fachexperten möglich, tiefer in die Risikoanalyse einzusteigen. Dies kann beispielsweise in Form von Workshops geschehen, bei denen die Fachteams die Risikoarten innerhalb ihres Fachgebiets näher erörtern. Ein Verantwortlicher aus dem Kernteam sollte hierbei die Rolle des Moderators übernehmen, um die Diskussion gezielt zu lenken. Der Projektleiter sollte die Ergebnisse der einzelnen Fachteams schließlich innerhalb seines Kernteams zusammenführen.

Die Risikoidentifikation sollte mit größter Sorgfalt geschehen, denn sie legt den Grundstein für eine einwandfreie Projektplanung und einen erfolgreichen Projektverlauf. Ist die Risikoidentifikation abgeschlossen, können mit den Fachteams gegenseitige Abhängigkeiten unter den Risiken und der Einfluss der Risiken auf den Business Case analysiert werden (vgl. hierzu Gausling, 2017b).

Fazit

In diesem Artikel wurde mit den 4 Os zur Risikoidentifikation ein Konzept vorgestellt, mit dem sich Risiken in Großprojekten systematisch und vollständig erfassen lassen. Es fasst eine Vielzahl verschiedener Risikokataloge und die darin vorkommenden Risikokategorien aus Literatur und Praxis in einem einzelnen und umfassenden Risikokatalog zusammen. Dabei stehen die 4 Os für operative, organisatorische, ökonomische und

ortsabhängige Risiken. Indem der Artikel klare Definitionen für die einzelnen Risikoarten aufzeigt und diese mit konkreten Projektbeispielen aus realen Großprojekten wie dem Biocéánico, der Elbphilharmonie oder Stuttgart 21 veranschaulicht, fördert er ein eindeutiges Verständnis möglicher Risikoarten in Großprojekten.

Literatur

- Ägypten Magazin (2018): Suezkanal, abrufbar unter: <http://www.aegypten-magazin.de/staedte/suezkanal/>, letzter Abruf: 10.07.2018.
- Balser, M. (2014): Wüstenstrom-Projekt Desertec zerfällt, Süddeutsche Zeitung vom 14.10.2014, abrufbar unter: <http://www.sueddeutsche.de/wirtschaft/wuestenstrom-projekt-endgueltiges-aus-fuer-desertec-1.2172778>, letzter Abruf: 10.07.2018
- Böttcher, J.; Blattner, P. (2013): Projektfinanzierung: Risikomanagement und Finanzierung, 3. Aufl., Oldenbourg Verlag, München 2013
- Conrad, N. (2015): Ein Kanal, der die Welt verzaubert, DW vom 05.08.2015, abrufbar unter: <http://www.dw.com/de/ein-kanal-der-die-welt-verzaubert/a-18631056>, letzter Abruf: 10.07.2018
- DESERTEC Foundation (2015): DESERTEC Foundation – Die DESERTEC Stiftung verlässt das Industriekonsortium Dii, abgerufen unter der URL: <http://www.desertec.org/de/presse/pressemitteilungen/130701-die-desertec-stiftung-verlaesst-das-industriekonsortium-dii/>, letzter Abruf: 12.01.2015
- Dii GmbH (2015): Unsere Mission, abgerufen unter der URL: <http://www.dii-eumena.com/de/ueber-uns.html>, letzter Abruf: 12.01.2015
- DIN SPEC 91331:2015-11, Klassifikation von Risiken für internationale Großprojekte
- Fiedler, J.; Wendler, A. (2015): Large Infrastructure Projects in Germany – Between Ambition and Realities. Public Infrastructure Project Planning in Germany: The Case of the BER Airport in Berlin-Brandenburg, Working Paper 3, Hertie School of Governance 2015
- Flyvbjerg, Bent (2014): What You Should Know About Megaprojects and Why: An Overview, in: Project Management Journal, Vol. 45 (2), 2014, S. 6-19
- Frankfurter Allgemeine Zeitung (2014): Der Traum vom Wüstenstrom ist gescheitert, FAZ am 14.10.2014, abrufbar unter: <http://www.faz.net/aktuell/wirtschaft/wirtschaftspolitik/wuestenstrom-projekt-desertec-ist-gescheitert-13207437.html>, letzter Abruf: 10.07.2018
- Gausling, P. (2016): Bewertung und Management von Risiken internationaler Großprojekte. Eine Untersuchung des Einflusses der Partitionierung auf die Risikosituation internationaler Großprojekte am Beispiel der Fallstudie DESERTEC, Verlag Dr. Kovač, Hamburg

- Gausling, P. (2017a): Der Ozean-Express: Zukunftsvision oder Größenwahn?, Projekt Magazin vom Apr/2017, abrufbar unter: https://www.projektmagazin.de/meilenstein/projektmanagement-blog/der-ozean-express-zukunftsvision-oder-groessenwahn_1119355, letzter Abruf: 10.07.2018
- Gausling, P. (2017b): **Abbildung von Risiken in Großprojekten oder was Risiken und Cocktails gemeinsam haben**, in: Projekt Magazin Vol. 18/2017, S. 1-15
- Hoegle, M. (2005): Smaller teams – better teamwork: How to keep project teams small, in: Business Horizons (2005), Vol. 48, 2005, S. 209-214
- Metzner, T. (2017a): Flughafen BER - beim Brandschutz hapert's immer noch, Der Tagesspiegel am 06.07.2017, abrufbar unter: <http://www.tagesspiegel.de/berlin/hauptstadtflughafen-fluchhafen-ber-beim-brandschutz-haperts-immer-noch/20030234.html>, letzter Abruf: 10.07.2018
- Metzner, T. (2017b): Risiken und Nebenwirkungen des neuen Eröffnungstermins, Der Tagesspiegel am 15.12.2017, abrufbar unter: <http://www.tagesspiegel.de/berlin/hauptstadtflughafen-ber-risiken-und-nebenwirkungen-des-neuen-eroeffnungstermins/20714760.html>, letzter Abruf: 10.07.2018
- Niklas, Cornelia: Methodensteckbrief zur Risikoidentifikation, Projekt Magazin vom 22.10.2017, abrufbar unter: <https://www.projektmagazin.de/methoden/risikoidentifikation>
- Nord Stream AG (2013): Secure Energy for Europe. The Nord Stream Pipeline Project, 2005-2012, Grafenauweg
- Pollio, G. (1999): International Project Analysis and Financing, Macmillan Press, Houndmills
- Ritter, J.; Müssgens, C. (2013): Zeugnis des Schreckens, FAZ vom 15.11.2013, abrufbar unter: <http://www.faz.net/aktuell/wirtschaft/elbphilharmonie-zeugnis-des-schreckens-12666153.html>, letzter Abruf: 10.07.2018
- Spiegel (2017): Woche der Wahrheit für Stuttgart 21, Spiegel vom 12.12.2017, abrufbar unter: <http://www.spiegel.de/wirtschaft/unternehmen/stuttgart-21-bei-der-sondersitzung-der-bahn-soll-es-um-die-neuen-risiken-gehen-a-1182809.html>, letzter Abruf: 10.07.2018
- Spiegel (2018): Kosten für BER übersteigen sieben Milliarden Euro, Spiegel vom 23.02.2018, abrufbar unter: <http://www.spiegel.de/wirtschaft/soziales/flughafen-berlin-brandenburg-ber-kosten-steigen-auf-7-3-milliarden-euro-a-1195101.html>, letzter Abruf: 10.07.2018ss
- Tinsley, C. R. (2000): Advanced Project Financing: Structuring Risk, Euromoney Books, London
- Yescombe, E. R. (2014): Principles of Project Finance, 2. Aufl., Elsevier Science, Burlington