Risiko-Management beim Outsourcing von IT

Diplomarbeit

Studiengang Informationswirtschaft

der

Fachhochschule Stuttgart –

Hochschule der Medien

Stavroula Vassia

Erstprüferin: Prof. Dr. Bettina Schwarzer

Zweitprüferin: Prof. Margarete Payer

Bearbeitungszeitraum: 03.05.2004 bis 03.09.2004

Stuttgart, September 2004

Kurzfassung

Das Outsourcing der IT erfreut sich in unserer heutigen Zeit einer immer größeren Beliebtheit. Chancen, wie Kostenreduzierung, Vermeidung von Kapazitätsengpässen und Konzentration auf die Kerngeschäfte werden damit verbunden. Die Vorgehensweise ist dabei die Verantwortung des Ganzen oder Teilen des IT-Betriebs auf ein anderes, externes Unternehmen zu verlagern. Diese Vorgehensweise ist nicht nur mit Chancen verbunden, sondern auch mit Risiken. Werden diese Risiken ignoriert und keine Gegenmaßnahmen ergriffen, können sie zu einer Gefahr für die erfolgreiche Realisierung des IT-Outsourcing-Projekts werden. Die Begleitung des IT-Outsourcing-Projekts durch das Risiko-Management gewinnt deshalb an Bedeutung und wird zunehmend als Erfolgsfaktor betrachtet. Es ermöglicht nämlich den systematischen Umgang mit den Risiken des IT-Outsourcings.

Schlagwörter: IT-Outsourcing, Risiko-Managment, Risiken, Risikoleitfaden

Abstract

The outsourcing of the IT enjoys a bigger and bigger popularity in our time of today. Chances, like cost reduction, avoidance of capacity bottlenecks and concentration on the core business are connected with that. The modus operandi is thereby to shift the responsibility of the whole or parts of the IT operation on another external enterprise. This modus operandi isn't only connected to chances but also to risks. If these risks are ignored and no countermeasures taken up, they can become a danger for the successful realization of the IT outsourcing project. The company of the IT outsourcing project by the risk management therefore becomes more important and is increasingly regarded as a success factor. It allows namely systematic dealing with the risks of the IT outsourcing.

Keywords: it outsourcing, risk management, risks, risk guide

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

GmbH	Gesellschaft mit begrenzter Haftung
IM	InformationsManagement
IT	Informationstechnologie
ITRM	IT-Risiko-Management
LoI	Letter of Intent
KonTraG	Gesetz zur Kontrolle und Transparenz
RWK	Risiko-Wahrscheinlichkeitsklasse
SLA	Service Level Agreement

1 Einleitung

1.1 Problemstellung und Ziel der Arbeit

1.1.1 IT-Outsourcing – Chance und Risiko

In einer zunehmend komplexen Welt mit immer kürzeren Produktlebenszyklen, einer immer größeren Vielzahl an Technologien, Konkurrenzdruck und immer höheren Marktanforderungen, geraten viele Unternehmen unter Druck. Um diesen Anforderungen zu begegnen und wettbewerbsfähig zu bleiben, sind viele Unternehmen auf der Suche nach Möglichkeiten, die Komplexität ihres täglichen Geschäfts zu senken, ihre Geschäftsabläufe zu optimieren und dabei möglichst Kosten sparen. Ein Outsourcing der Informationstechnologie bietet dafür vielen Unternehmen einen Lösungsweg. Sie können sich auf ihr Hauptgeschäft konzentrieren, ohne von Supportprozessen, wie dem IT-Betrieb, gestört zu werden, zumal viele Unternehmen keinen Überblick über ihre IT haben und den neuen Entwicklungen im IT-Bereich nicht hinterherkommen. Die IT stellt für viele Unternehmen deshalb eine Belastung dar. Die Überlegung durch ein Outsourcing die Verantwortung des IT-Bereichs oder Teile davon auf einen Spezialisten, also einen IT-Dienstleister, zu übertragen liegt da nahe. Auch der Kostenaspekt spielt dabei eine Rolle. Ein Outsourcing der IT stellt nämlich in vielen Fällen eine kostengünstigere Alternative als der interne Betrieb der IT dar.

Bei allen Chancen, die sich durch ein IT-Outsourcing für ein Unternehmen ergeben, sollte nicht übersehen werden, dass ein Outsourcing der IT auch Risiken birgt. Schon seit vielen Jahren ist die Bedeutung der Informationstechnologie für die Geschäftstätigkeit von Unternehmen klar geworden. Es wird heutzutage sogar immer öfter davon gesprochen, IT wertsteigernd einzusetzen. Die Abhängigkeit vom Funktionieren der IT wird für viele Unternehmen immer größer. Bricht der IT-Betrieb auch nur für wenige Stunden zusammen, können enorme finanzielle Verluste entstehen. Daraus ergeben sich enorme Risiken für das auslagernde Unternehmen. Nicht zu vergessen ist nämlich, dass ein Outsourcing der IT eine längere Partnerschaft mit einem externen Unternehmen bedeutet. Unternehmen, die Leistungen ausgelagert haben, sind dadurch von der Qualität der Leistungserbringung durch den Outsourcingnehmer abhängig. Zudem kommen Risiken bei der Übertragung der IT von einem Unternehmen zum anderen hinzu. Auch ist ein Outsourcing der IT nicht in allen Fällen möglich. Gehört die IT zum Kerngeschäft eines Unternehmens, kann ein Outsourcing zu einem Abfluss an wichtigem Know-how und Verlust an Fähigkeiten führen, die das Unternehmen schwächen oder sogar gefährden.

Ein Unternehmen, das seine IT ausgelagert hat, unterliegt also einer Vielzahl von Risiken, die vor der Realisierung eines solchen Vorhabens Beachtung finden sollten.

Schließlich wollen Unternehmen durch ein Outsourcing der IT Vorteile erlangen und nicht die internen Probleme beim Betrieb der IT mit Problemen, die durch das Outsourcing entstanden sind, eintauschen.

1.1.2 Die Bedeutung des Risiko-Managements und Ziel der Arbeit

Risiken sind ein Bestandteil der Geschäftstätigkeit eines jeden Unternehmens und bedeuten gleichzeitig Gefahr und nötige Voraussetzung für unternehmerischen Erfolg. Grund dafür ist, dass sich neue Chancen für Unternehmen oft erst durch das Eingehen von Risiken ergeben. Die Herausforderung liegt also in der bewussten Auseinandersetzung mit Risiken dort, wo auch gleichzeitig Chancen wahrgenommen werden können.

So sind auch mit einem neuen unternehmerischen Vorhaben, wie dem IT-Outsourcing, sowohl Chancen als auch Risiken verbunden. Die Risiken dabei zu ignorieren ist keine Lösung. Vielmehr ist ein kontrollierter Umgang mit Risiken erforderlich. Das Risiko-Management hat sich als Antwort auf diese Herausforderungen etabliert und kann als Konzept zur Bewältigung von Bedrohungen, die das ganze Unternehmen betreffen, verstanden werden. Das schließt Risiken mit ein, die von komplexen Projekten, wie dem IT-Outsourcing, stammen. Durch das Risiko-Management können potenzielle Gefährdungssituationen frühzeitig erkannt und erfasst werden, sowie eingegrenzt und als bewusste Steuerungsgröße eingesetzt werden.

Ziel der vorliegenden Arbeit wird deshalb sein, die Bedeutung des Risiko-Managements für ein IT-Outsourcing klar zu machen. Zu diesem Zweck wird ausführlich auf die Risiken eingegangen, die mit einem solchen Vorhaben verbunden sind. Die Notwendigkeit der Begleitung eines IT-Outsourcing-Vorhabens durch das Risiko-Management kann dadurch verdeutlicht werden. Der Nutzen, der durch ein Outsourcing der IT entstehen kann, soll dabei keineswegs geschmälert werden.

Der zweite wesentliche Schwerpunkt dieser Arbeit beschäftigt sich damit, die wichtigsten Schritte aufzuzeigen, die zur Einbeziehung und Durchführung des Risiko-Managements in IT-Outsourcing-Projekten gemacht werden müssen. Dies wird in Form eines Leitfadens stattfinden.

1.2 Aufbau der Arbeit

Die vorliegende Arbeit beschäftigt sich mit dem Risiko-Management, das für ein Outsourcing der IT erforderlich ist. Dabei wird die Arbeit in vier wesentliche Teile unterteilt sein.

Im ersten Teil werden die Grundlagen des IT-Outsourcings erläutert. Zunächst wird dabei auf die Formen des IT-Outsourcings eingegangen und welche Nutzenpotenziale damit verbunden sind. Anschließend wird erläutert, welche strategischen Entscheidungen im Vorfeld des IT-Outsourcings getroffen werden müssen und wie die Vertragsgestaltung aussieht.

Den Abschluss dieses Teils bildet die Vorgehensweise bei der Durchführung von IT-Outsourcing-Projekten. Dabei soll auch auf die Wechselwirkung zwischen Projekt- und Risiko-Management eingegangen werden.

Nachdem im ersten Teil die Grundlagen des IT-Outsourcings geklärt wurden, soll beleuchtet werden, welche Risiken mit einem solchen Vorhaben verbunden sind. Dazu werden die Risiken kategorisiert und ausführlich erläutert. Darüber hinaus wird zu Beginn dieses Teils auf die gesetzliche Verpflichtung zur Risikoerfassung aufmerksam gemacht werden.

Aufbauend auf der Darstellung der Risiken soll im dritten Teil das Risiko-Management als Möglichkeit zum Umgang mit Risiken vorgestellt werden. Dazu sollen allgemeine Grundlagen, wie die Risikokultur, der Risiko-Management-Prozess und die Risikodokumentation, erläutert werden. Ferner wird auf das IT-Risiko-Management und seine Bedeutung in der Outsourcing-Thematik eingegangen. Zum Abschluss dieses Teils werden noch weitere an das Risiko-Management angelehnte Techniken vorgestellt werden, die dann eine Rolle spielen, wenn das Risiko-Management gescheitert ist.

Der vierte Teil bildet schließlich den Schwerpunkt dieser Arbeit. Inhalt dieses Teils ist die Entwicklung eines Leitfadens für ein Risiko-Management beim Outsourcing der IT. Durch den Leitfaden werden die Schritte erläutert, die für ein Risiko-Management in IT-Outsourcing-Projekten gemacht werden müssen. Dazu wird der Leitfaden in zwei Teile aufgesplittet. Im ersten Teil wird auf die Rahmenbedingungen eingegangen, die für ein Risiko-Management in IT-Outsourcing-Projekten benötigt werden. Der zweite Teil wird schließlich den Risiko-Management-Prozess zum Mittelpunkt haben und soll eine Möglichkeit zur Durchführung des Risiko-Managements in IT-Outsourcing-Projekten darstellen.

Nach dem vierten Teil wird kurz auf die Auswirkungen, die ein IT-Outsourcing auf den Outsourcinggeber hat eingegangen. Dieser Teil wird nicht ausführlich behandelt. Es soll lediglich kurz aufgezeigt werden, dass mit dem Outsourcing der IT Auswirkungen und Veränderungen beim Outsourcinggeber verbunden sind. Anschließend wird in einem Exkurs auf die Gründe eingegangen, die IT-Outsourcing-Projekte zum Scheitern bringen können.

Die spezifischen Aufgaben des Projekt-Managements werden im Rahmen dieser Arbeit nicht ausführlich behandelt werden. Der Schwerpunkt wird beim IT-Outsourcing und beim Risiko-Management liegen.

2 Grundlagen des IT-Outsourcing

2.1 Begriffsklärung und Möglichkeiten zur institutionellen Einbindung des IT-Outsourcing

Der Begriff Outsourcing ist ein Kunstwort, der sich ausgehend vom Wortstamm, aus den drei englischen Wörtern „Outside", „Ressource" und „Using" zusammensetzt. Wörtlich übersetzt bedeutet er zunächst „Nutzung externer Ressourcen" (vgl. Schätzer 199, S.43). Eine einheitliche Definition des Begriffes Outsourcing ist in der Literatur nicht zu finden. Dies liegt zum einen daran, dass ein großer Teil der Outsourcing-Literatur aus Fallstudien von Praktikern besteht, die keine inhaltliche Klärung des Begriffes vornehmen, zum anderen aber auch daran, dass aufgrund unterschiedlicher Abgrenzung des Gegenstandsbereiches durch die Autoren bei wissenschaftlichen Abhandlungen eine Fülle an unterschiedlichen Definitionen zu finden sind. Exemplarisch sollen an dieser Stelle zwei Definitionen vorgestellt werden:

Zahn, Barth und Hertweck verstehen unter Outsourcing *„den Prozess der Auslagerung von bislang im Unternehmen erbrachten Leistungen an einen externen Dritten. Diesem wird dabei die dauerhafte unternehmerische Verantwortung für eine sachgerechte Leistungserstellung übertragen"* (Zahn/Barth/Hertweck 1998, S.7).

Laut Bullinger, Rüger und Thiele bringt das Wort Outsourcing zum Ausdruck, dass *„eine beliebige Unternehmensfunktion auf ein anderes Unternehmen übertragen, und damit der Grad der vertikalen Integration oder Betriebs- bzw. Leistungstiefe reduziert wird"* (Bullinger/Rüger/Thiele 1997, S.19).

In der Literatur lässt sich im Zusammenhang mit Outsourcing auch der Begriff Fremdbezug[1] finden. Im klassischen Sinn versteht man unter Fremdbezug die Beschaffung von Gütern und Leistungen, die nicht im Unternehmen selbst erstellt werden. Beim Outsourcing hingegen werden Leistungen ausgelagert, die bisher im Unternehmen erbracht wurden, aber in Zukunft extern bezogen werden sollen. Outsourcing kann demnach als eine spezielle Form von Fremdbezug gesehen werden (vgl. Zahn/Barth/Hertweck 1998, S.7).

Stellt ein Unternehmen Überlegungen an, interne Leistungen auszulagern, muss es sich über die institutionelle Einbindungsform des Outsourcings Gedanken machen. Je nachdem, für welche institutionelle Einbindungsform man sich entscheidet, wird nämlich auch die Stärke der Zusammenarbeit und Bindung an einen externen Partner unmittelbar mitentschieden.

[1] Im englischen Sprachgebrauch als Make-or-Buy bezeichnet

Das Spektrum an Alternativen, das den Unternehmen bei der Suche nach einer geeigneten institutionellen Einbindung von Outsourcing-Partnern zur Verfügung steht, wird durch Abbildung 1 verdeutlicht.

Eigen-fertigung	**internes Outsourcing**				**externes Outsourcing**		
Eigen-erstellung	Center-Konzep-tion	Koopera-tion	Gemein-same Service-gesell-schaft	Kapital-beteili-gung	Lang-fristige Zusam-men-arbeit	Kurz-/ Mittel-fristige Zusam-men-arbeit	Spontane Zusam-men-arbeit

zunehmend hierarchische Koordination

zunehmend marktliche Koordination

Abbildung 1: Systematik von Outsourcing-Varianten (Quelle: Zahn/Barth/Hertweck 1998, S.9)

In der Abbildung werden die beiden Möglichkeiten[2] internes Outsourcing und externes Outsourcing unterschieden. Um bei einer Leistungserbringung von externem Outsourcing sprechen zu können, müssen mindestens drei Kriterien erfüllt sein (vgl. Zahn/Barth/Hertweck 1998, S.8). Zunächst muss es sich bei der Übertragung der Leistungen um einen längerfristigen Zeitraum handeln - im Extremfall um einen permanenten. Zum anderen sollte eine „spezifische, individuelle Form der Zusammenarbeit“ (Zahn/Barth/Hertweck 1998, S.8) zu finden sein. Das bedeutet, dass jedes Outsourcing-Vorhaben verschieden ist und unterschiedliche Merkmale aufweist[3]. Als drittes Kriterium wird die Marktbezogenheit des Vorhabens genannt.

Es sollte also mindestens ein externes Unternehmen, das wirtschaftlich und rechtlich eigenständig ist und Geschäftsbeziehungen zu weiteren Unternehmen pflegt, an dem Prozess beteiligt sein (vgl. Zahn/Barth/Hertweck 1998, S.8). Damit kann man externes von internem Outsourcing klar voneinander abgrenzen. Die späteren Ausführungen, die im Rahmen dieser Arbeit gemacht werden, richten sich auf das externe IT-Outsourcing.

[2] Die dritte Alternative in der Abbildung, die Eigenfertigung, wird in Kapitel 2.4.1 erläutert.

[3] Ein Beispiel dafür ist die individuelle Vertragsgestaltung.

2.2 Klassische Formen des IT-Outsourcings und Application Service Providing

In der Praxis haben sich sehr unterschiedliche Formen des externen Outsourcings herausgebildet. Die vier häufigsten Formen des IT-Outsourcing sind nach Söbbing die Konzentration von IT-Aktivitäten im Unternehmen, konzerninternes Outsourcing, totales Outsourcing und partielles Outsourcing[4] (vgl. Söbbing 2002, S. 25).

Bei der Konzentration von IT-Aktivitäten kann man die beiden Fälle Konzentration von IT-Aktivitäten im Unternehmen und Konzentration von IT-Aktivitäten im Konzern unterscheiden. Im ersten Fall werden die IT-Service-Aktivitäten mit Hilfe eines externen Dienstleisters zu einer Fachabteilung im Unternehmen zusammengefasst. Dieser Vorgang kann auch intern geregelt werden, ohne einen externen Dienstleister heranzuziehen. Für diese Aufgabe kann beispielsweise eine interne Fachabteilung herangezogen werden. Da in diesem Fall aber alle Funktionen im Unternehmen verblieben, spricht man nicht mehr von externem Outsourcing (vgl. Söbbing 2002, S. 27).

Vom zweiten Fall, dem konzerninternem Outsourcing, spricht man, wenn die IT-Service-Aktivitäten aller Abteilungen des Konzerns in einem Beteiligungsunternehmen gebündelt werden. IT-Service-Aktivitäten an den Konzern werden dann von diesem Beteiligungsunternehmen (Joint Venture) erbracht. Es besteht auch die Möglichkeit die IT-Service-Aktivitäten in einem Tochter- oder Gemeinschaftsunternehmen zu konzentrieren. Im Gegensatz zu Beteilgungsunternehmen ist bei diesen beiden Fällen allerdings kein externer Outsourcing-Anbieter beteiligt, so dass das Kriterium der Marktbezogenheit nicht erfüllt ist und man von internem IT-Outsourcing sprechen muss (vgl. Söbbing 2002, S. 28).

Totales Outsourcing beschreibt die vollständige Auslagerung eines Leistungsbereichs eines Unternehmens oder Konzerns an ein externes Unternehmen. Im Falle des IT-Outsourcing bedeutet das beispielsweise die gesamte Auslagerung des IT-Betriebs (vgl. Söbbing 2002, S. 33).

Im Gegensatz zum totalen Outsourcing bedeutet das partielle Outsourcing die Auslagerung eines bestimmten Teils einer Leistung an ein Drittunternehmen. Im Zusammenhang mit dem IT-Outsourcing bedeutet das die Auslagerung nur eines Teils des IT-Betriebs.

Es gibt auch die Möglichkeit des so genannten Multisourcings, bei dem beispielsweise der gesamte IT-Betrieb fremdvergeben werden soll. Dies geschieht dann aber nicht in Form eines totalen Outsourcing mit nur einem einzigen Outsourcing-Anbieter.

---

[4] Auch zu erwähnen ist das Business Process Outsourcing. In diesem Fall findet eine Auslagerung eines gesamten Unternehmensprozesses inklusive der dazu gehörenden IT und Sachbearbeiterleistung statt. Der Outsourcinggeber bezieht dadurch das Prozessergebnis, ohne in den Verantwortungsbereich oder die Infrastruktur des ausgelagerten Unternehmensprozesses miteinbezogen zu werden.

Man bedient sich beim Multisourcing verschiedener Outsourcing-Anbieter, die jeweils einen Teil der Leistung übernehmen (vgl. Söbbing 2002, S. 47).

Die verschiedenen Outsourcing-Formen haben jeweils Vor- und Nachteile[5] und unterscheiden sich in Bezug auf die Stärke der Zusammenarbeit und Bindung an einen externen Partner, und ebenso in der Höhe der Anforderungen. Allgemein lässt sich folgendes festhalten: Je stärker die Bindung an einen externen Partner ist, desto höher sind auch die Anforderungen, die sich an das Outsourcing-Projekt richten.

Abbildung 2 verdeutlicht den Zusammenhang zwischen der Höhe der Anforderungen und der Outsourcing-Form.

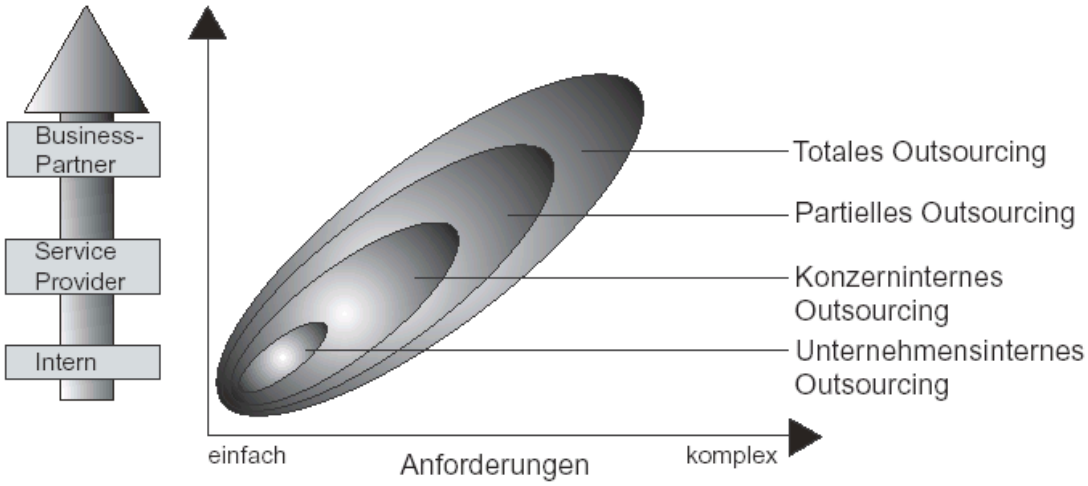


Abbildung 2: Outsourcing-Form und Anforderungen (Quelle: Söbbing 2002, S. 25)

Abgesehen von den genannten Outsourcing-Formen findet man in der Outsourcing-Terminologie heutzutage auch andere Varianten des externen IT-Outsourcings.

Es sollten deshalb auch die IT-Outsourcing-Modelle Application Hosting und ASP (Application Service Providing) erwähnt werden. Unter ASP versteht man einen Dienstleister, der einzelne Anwendungen und Software für seinen Kunden auf seinen eigenen Systemen betreibt. Die Anwendungen können dabei auf einem zentralen Server zur Verfügung stehen und über das Internet oder Virtual Private Networks (VPN) von den Unternehmen abgerufen werden. Beim Application Hosting ist ebenfalls der Betrieb von Anwendungen an einen Dienstleister ausgelagert.

[5] Auf die Vor- und Nachteile jeder einzelnen Form wird nicht eingegangen, da es den Rahmen der Diplomarbeit sprengen würde. Auch in der weiterführenden Literatur wird in der Regel nicht auf die Vor- und Nachteile der einzelnen Outsourcing-Formen eingegangen, sondern ein allgemeiner Überblick vermittelt. Zu einem allgemeinen Überblick über Nutzen und Risiken des IT-Outsourcings vgl. Kapitel 2.3 und Kapitel 3

Im Gegensatz zum ASP-Modell gehören die Anwendungen allerdings noch dem jeweiligen Kunden (vgl. http://www.bsi.de/gshb/deutsch/menue.htm). Die Grenzen zwischen klassischem Outsourcing und reinem ASP verschwinden in der Praxis zunehmend. Aus diesem Grund wird im Folgenden nur noch allgemein von IT-Outsourcing die Rede sein.

2.3 Motivation und Nutzenpotentiale

Ein Outsourcing der IT ist eine Entscheidung, die das gesamte Unternehmen betreffen kann. Sie ist damit von strategischer Bedeutung und sollte deshalb von der verantwortlichen Ebene (Geschäftsführung/Vorstand) getroffen werden, zumal Outsourcing-Projekte mit erheblichen Risiken verbunden sind und u.U. Umstrukturierungsmaßnahmen nach sich ziehen können. Bei Auslagerungsunwilligkeit der verantwortlichen Ebene kann ein IT-Outsourcing-Projekt nicht durchgeführt werden (vgl. Pastors 2002, S.492).

Die Gründe für ein Unternehmen, an IT-Outsourcing zu denken, können dabei sehr vielfältig sein. Der Anstoß zu einer IT-Outsourcing-Überlegung kann operativer also kurzfristiger Natur sein, aber auch strategische und demnach langfristige Beweggründe haben. Waren in der Vergangenheit hauptsächlich kurzfristig orientierte operative Aspekte, wie Kostenreduzierung und Beseitigung von Kapazitätsengpässen, die treibende Kraft für ein Outsourcing der IT, treten heute strategische Aspekte, wie die Fokussierung auf den Nutzwert oder Business Value eines Unternehmens, zunehmend in den Vordergrund (vgl. Köhler-Frost 2002, S. 90).

Durch die Auslagerung von unwesentlichen Rand- oder Unterstützungsaktivitäten der Wertschöpfung, können sich die Unternehmen auf ihre besonderen Stärken, ihre Kerngeschäftsfelder, konzentrieren. Sie erhalten so die Möglichkeit sich langfristig besser auf die Markt- und Wettbewerbserfordernisse auszurichten, und damit ihre Ertragsentwicklung nachhaltig zu verbessern. IT-Outsourcing hat sich dadurch zunehmend zu einem akzeptierten Management-Instrument der strategischen Unternehmensführung gewandelt.

	Outsourcing der Informationstechnologie entwickelt sich zu einem akzeptierten Management-Werkzeug
Traditionell	▪ Einsparen oder variabilisieren von IT-Kosten ▪ Steigerung von Performance, Kapazität und Qualität
Service / Dienstleister	▪ Zutritt zu den Ressourcen eines globalen Dienstleisters ▪ Vereinfachter Zutritt zu globalen Märkten durch neue Technologien und bestehender lokaler Präsenz des Dienstleisters
Business Value	▪ Nutzung der Informationstechnologie zur Identifikation und Realisierung von Wertschöpfungspotentialen im Unternehmen oder zur Verbesserung der Marktposition ▪ Strukturwandel von traditioneller vertikaler Organisation zu flexibler Organisationsstruktur rund um die Kernkompetenzen ▪ Neudefinition, Fokussierung & Vitalisierung des Unternehmens

Abbildung 3: Outsourcing im Wandel (Quelle: Köhler-Frost 2002, S. 91)

Nichtsdestotrotz werden auch heute noch Outsourcing-Überlegungen vor allem aus operativen Motiven heraus gemacht. Immer noch ist der am häufigste genannte Grund für ein Outsourcing der IT die Kostenreduzierung. Weitere Motive für ein IT-Outsourcing bilden für Unternehmen die damit verbundenen Nutzenpotenziale. Die wichtigsten Nutzenaspekte des Outsourcing von IT lassen sich wie folgt zusammenfassen:

- Konzentration auf die Kernkompetenzen: Bestimmte Dienstleistungen der eigenen IT-Produktion, wie etwa der Betrieb der Infrastruktur, sind für viele Unternehmen ein fester Bestandteil ihrer IT. Sie gehören jedoch nicht zu den Kernkompetenzen eines Unternehmens und tragen nicht unmittelbar zu einem Gewinn bei. In solchen Fällen bietet das IT-Outsourcing die Möglichkeit, sich auf die tatsächlich strategisch relevanten, wertschaffenden IT-Aktivitäten zu konzentrieren und so die Komplexität der intern zu erbringenden Leistungen zu reduzieren (vgl. Buchta/Eul/Schulte-Croonenberg 2004, S.186).
- Konsolidierung: In vielen Unternehmen besteht keine einheitliche IT-Landschaft. Vielmehr haben die unterschiedlichen Geschäftsbereiche ihre eigene auf ihren Interessen aufgebaute und meist historisch gewachsene IT-Landschaft. IT-Outsourcing bietet hier die Möglichkeit, Einzelinteressen zu durchbrechen und eine Konsolidierung der IT-Landschaft aus Gesamtsicht zu erzwingen. Die nötigen Restrukturierungen können somit beschleunigt werden (vgl. Buchta/Eul/Schulte-Croonenberg 2004, S.186).
- Substitution von Fixkosten durch variable Kosten: Dieses Phänomen entsteht beispielsweise, wenn der IT-Outsourcing-Anbieter die erbrachten IT-Dienstleistungen nach der abgenommenen Menge abrechnet, z.B. pro Arbeitsplatz oder gar pro Geschäftstransaktion. Die ehemals fixe Ressource IT verwandelt sich so in eine an die Geschäftstätigkeit angepasste Variable (vgl. Buchta/Eul/Schulte-Croonenberg 2004, S.187).

- Substitution von Personalabhängigkeit durch vertragliche Partnerschaften,
- IT-Bedarf, IT-Leistung und resultierende IT-Kosten können transparent gemacht werden,
- Zugriff auf bewährte und dem neuesten Stand der Technik entsprechende IT-Ressourcen des Anbieters,
- Effizientere Nutzung der IT-Ressourcen,
- Beschaffungsprobleme qualifizierter IT-Kräfte werden vermieden,
- Nutzung des Know-how von spezialisierten Dienstleistern, beispielsweise bei der Installation und Wartung von Hard- und Software,
- Erhöhung des Dienstleistungsniveaus durch höhere Servicequalität,
- Risikoverteilung und –begrenzung (vgl. Köhler-Frost 2002, S.128).

2.4 Strategische Entscheidungen im Vorfeld des IT-Outsourcings

2.4.1 Make-or-Buy

Wie im vorangegangenen Kapitel deutlich wurde, werden mit dem Outsourcing der IT eine ganze Reihe an Nutzenpotenzialen verbunden. Die Überlegung IT auszulagern kann aus einer Notwendigkeit heraus entstehen. Aber auch Nutzenpotenziale, wie Kosteneinsparung, können den Beweggrund für Outsourcing-Überlegungen bilden. Es stellt sich für ein Unternehmen aber zunächst die Frage, ob ein Fremdbezug tatsächlich vorteilhafter als die Eigenerstellung ist. Diese Frage muss vor einer Durchführung eines Outsourcing-Projekts geklärt werden. Um eine Make-or-Buy-Entscheidung treffen zu können, muss geklärt werden, welche Leistungen nach außen vergeben werden können, ohne die Wissensbasis eines Unternehmens zu gefährden oder in eine gefährliche Abhängigkeit des Outsourcing-Dienstleisters zu geraten (vgl. Zahn, Barth, Hertweck 1998, S. 23). Die Identifikation von Kernkompetenzen ist deshalb eine wichtige Entscheidungshilfe. Kernkompetenzen zeichnen sich im wesentlichen durch vier Eigenschaften aus (Köhler-Frost 2002, S.106):

- „Sie umfassen einen wesentlichen Teil der Wertschöpfungskette.
- Sie sind schwer zu kopieren.
- Sie tragen viel zum Kundennutzen bei.
- Sie sind durch einen Lernprozess entstanden.“

Kernkompetenzen sind also durch Wissen begründete Fähigkeiten, die von Mitbewerbern nicht einfach kopiert oder nachgeahmt werden können. Durch sie kann sich ein Unternehmen am Markt und im Wettbewerb differenzieren. Es ist deshalb abzuraten, Kernkompetenzen auszulagern.

Durch die Identifikation von Kernkompetenzen ergibt sich also eine Unterscheidung von unbedingt selbst zu erstellenden sowie potenziell auszulagernden Leistungen. Letztgenannte werden auch als Outsourcing-Kandidaten bezeichnet (vgl. Zahn/ Barth/ Hertweck 1998, S. 70). Für ein Outsourcing kommen also grundsätzlich alle Steuerungs- und Unterstützungsfunktionen, die nicht zu den Kernfunktionen eines Unternehmens gehören oder einen entscheidenen Wettbewerbsvorteil schaffen in Frage. Dennoch müssen sie dadurch nicht zwangsläufig für ein Outsourcing geeignet sein.

Erst kostenrechnerische Verfahren und eine umfassende Chancen- und Risiken-Abwägung bilden eine Entscheidungsgrundlage. Ein mögliches kostenrechnerisches Verfahren ist der Preis-Kosten-Vergleich. Dabei werden die Kosten der Eigenerstellung mit dem Preis bei einem Fremdbezug verglichen. Um ein möglichst exaktes und realitätsnahes Ergebnis zu erhalten, sollten dafür nur die Kosten berücksichtigt werden, die tatsächlich betroffen sind. Es sind also nur solche Kosten einzurechnen, die bei Durchführung der beiden Alternativen, Fremdbezug oder Eigenerstellung, zusätzlich entstehen oder wegfallen.

Grundsätzlich lassen sich bei Preis-Kosten-Vergleichen zwei mögliche Gegebenheiten unterscheiden. Die eigenen Produktionskapazitäten sind entweder unterausgelastet oder voll ausgelastet. Sind die Produktionskapazitäten unterausgelastet tendieren die Unternehmen oft zur Make-Option, da die Fixkosten zunächst gleich bleiben und die „Leerkosten“ so gefüllt werden können. Für den Preis-Kosten-Vergleich bedeutet das also, dass zunächst nur die variablen Kosten heranzuziehen sind. Auf lange Sicht reicht jedoch lediglich das Heranziehen der variablen Kosten nicht aus, da sich auch die Kapazitätsauslastungen ändern können. Lang- bzw. kurzfristig erforderliche Kapazitätsanpassungen müssen bei der Kostenbetrachtung deshalb berücksichtigt werden (vgl. Müller/Prangenberg 1997, S.38).

Die Methode des Preis-Kosten-Vergleichs gehört zu den konventionellen kostenrechnerischen Verfahren und weist einige Unzulänglichkeiten auf. Es werden beispielsweise die Transaktionskosten, die beim Prozess des Übergangs der IT an einen externen Outsourcing-Partner entstehen, nicht berücksichtigt. Diese Kosten sollten für eine Make-or-Buy-Entscheidung miteinbezogen werden. Die unten stehende Tabelle gibt eine Übersicht über mögliche anfallende Transaktionskosten.

Kostenart	Beschreibung
▪ Anbahnungskosten	Suche nach potentiellen Dienstleistern und Feststellung ihrer Konditionen
▪ Vereinbarungskosten	Verhandlung, Vertragsformulierung
▪ Abwicklungskosten	Steuerung der laufenden Leistungserstellung
▪ Kontrollkosten	Überwachung der vertraglichen Vereinbarungen
▪ Anpassungskosten	Durchsetzung von Vertragsänderungen aufgrund geänderter Rahmenbedingungen

Tabelle 1: Transaktionskostenarten (Quelle: Pastors 2002, S.497 [Quelle: KPMG])

Außerdem wird beim Preis-Kosten-Vergleich die Minimierung der Kosten in den Mittelpunkt der Überlegungen gesetzt. Mögliche andere Beweggründe für ein IT-Outsourcing, wie Qualitätssteigerung durch Fremdbezug einer Leistung, bleiben unberücksichtigt, ebenso mögliche Risiken, wie Know-how-Verlust. Qualitative Verfahren, wie das Abfassen einer Argumentenbilanz, und die Nutzwertanalyse sollten deshalb parallel zu kostenrechnerischen Verfahren durchgeführt werden (vgl. Zahn, Barth, Hertweck 1998, S. 77f).

In bestimmten Fällen können qualitative Faktoren einen errechneten Kostenvorteil für ein IT-Outsourcing überkompensieren und eine Eigenerstellung sinnvoller machen. Das Abfassen einer Argumentenbilanz und eine Nutzwertanalyse können für eine solche Prüfung zweckmäßig sein. Bei der Argumentenbilanz werden Argumente, die für ein Outsourcing sprechen Argumenten, die gegen ein Outsourcing sprechen, gegenübergestellt.

Dabei werden strategische, personelle und leistungs- sowie kostenrelevante Aspekte berücksichtigt. Eine konkrete Bewertung kann mit Hilfe der Argumentenbilanz allerdings nicht erfolgen. Dies geschieht durch eine Nutzwertanalyse. Sie ermöglicht eine Bewertung von Alternativen unter Berücksichtigung auch solcher Kriterien, die sich nicht in quantitativ messbaren Größen, wie z.B. in Geldeinheiten, ausdrücken lassen. Mögliche Bewertungskriterien können dabei das Innovationspotential, die Leistungsstärke und Zuverlässigkeit, die Kostenposition und der Marktfokus sein. Ein Vorteil der Nutzwertanalyse ist, dass die einzelnen Schritte der Entscheidung transparent gemacht werden. Die folgende Abbildung verdeutlicht die Vorgehensweise bei der Nutzwertanalyse.

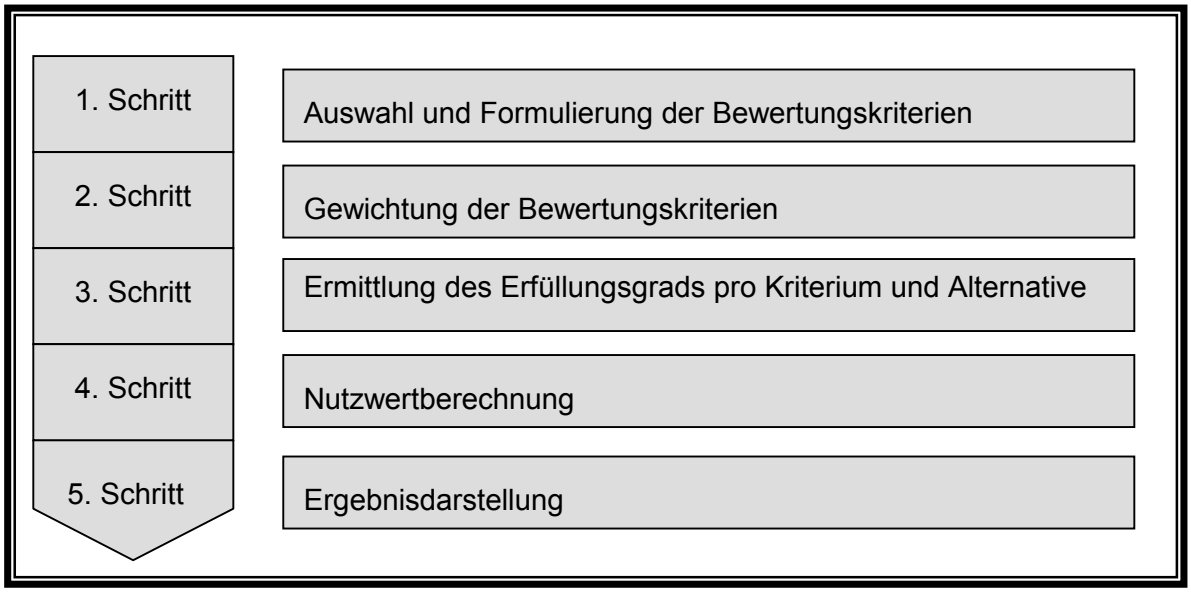


Abbildung 4: Grundsätzliche Vorgehensweise bei der Nutzwertanalyse (Quelle: Zahn, Barth, Hertweck 1998, S. 41)

Ein zentrales Problem qualitativer Bewertungsgrößen ist, dass es oftmals keine Eindeutigkeit der Aussagen gibt. Dieses Problem bleibt auch bei der Nutzwertanalyse bestehen. Die einzelnen Alternativen können hinsichtlich eines Kriteriums gegenläufige Tendenzen aufweisen oder gleichzeitig Vor- und Nachteile haben. Beispielsweise kann man durch ein Outsourcing der IT externes Know-how erschließen. Gleichzeitig begibt man sich aber auch in eine erhöhte Abhängigkeit zu einem Outsourcing-Dienstleister (vgl. Zahn, Barth, Hertweck 1998, S. 80).

Bei den qualitativen Kriterien sind auch die potentiellen Auslagerungs-Barrieren des IT-Outsourcings zu nennen. Dazu gehören z.B.:

- nötiges Know-how extern nicht verfügbar,
- hoher Koordinations- und Abstimmungsaufwand,
- hoher Einarbeitungsaufwand,
- anteilige Gemeinkosten nicht abbaubar und
- hoher Grad an Verbundenheit mit anderen Bereichen.[6]

Allgemein lässt sich sagen, dass Kostenvorteile durch bleibende Belastungen aus den Gemeinkostenbereichen, Transaktionskosten, Auslagerungs-Barrieren und strategischen Nachteilen zunichte gemacht werden können. Die Make-or-Buy-Entscheidung hilft Unternehmen, herauszufinden, ob ein Outsourcing der IT tatsächlich die erhofften Nutzenpotenziale bringt oder ob anderweitige Lösungen sinnvoller sind.

2.4.2 Auswahl des geeigneten Outsourcing-Providers

Hat man sich für ein Outsourcing der IT entschieden, ist eine detaillierte Partnersuche und –auswahl unumgänglich. Nur so lässt sich das Risiko von Fehltritten minimieren und die Outsourcing-Erwartungshaltung größtmöglich erfüllen. Eine Outsourcing-Partnerschaft bedeutet schließlich eine Zusammenarbeit über mehrere Jahre und entscheidet nicht zuletzt über den Erfolg eines Outsourcing-Vorhabens. Aufgrund des starken Wettbewerbs im IT-Dienstleistungsumfeld sind die Unternehmen heute in der Lage aus einer Vielzahl von Outsourcing-Providern zu wählen. Wegen des hohen Konkurrenzdrucks liegen dabei viele Angebote von IT-Providern sehr niedrig, in einigen Fällen so niedrig, dass sie nicht einmal ihre Investitionskosten wieder einspielen können.

Die Ansprüche an die Leistungsfähigkeit und Qualität des IT-Anbieters indes steigen und erfordern von ihm zur Erfüllung oftmals häufige Investitionen in die eigene IT-Infrastruktur und damit zusätzliche Kosten. Niedrigpreise und hohe Leistungsanforderungen können IT-Dienstleister so bis zum Zusammenbruch führen. Eine Entscheidung für einen Outsourcing-Provider allein aufgrund der Preisgünstigkeit ist deshalb nicht zu empfehlen.

---

[6] Weitere Auslagerbarrieren sind bei Müller / Prangenberg (1997) zu finden

Durch eine umfassende Partnersuche kann das Risiko, von einem solchen Szenario in Mitleidenschaft gezogen zu werden, verringert werden. Abbildung 5 zeigt einen möglichen Ablauf bei einer Partnerwahl.

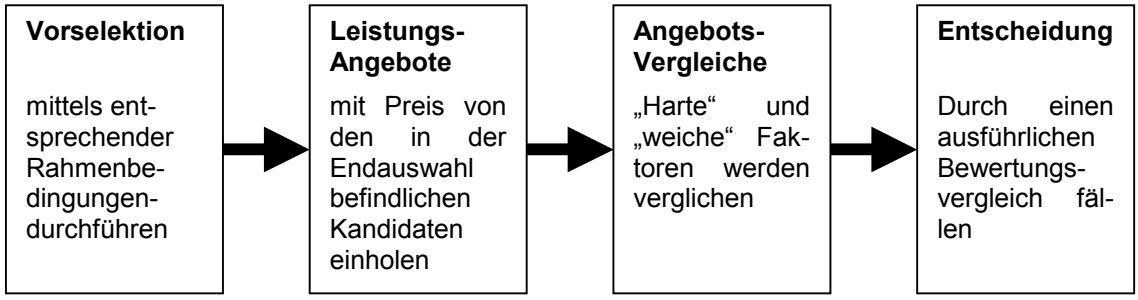


Abbildung 5: Ablauf Partnerauswahl (Quelle: Wißkirchen 1999, S. 215)

Die Faktoren bei einer Partnerwahl hängen vor allem von den jeweiligen spezifischen Anforderungen[7] eines Unternehmens ab. Ein möglichst detailliertes Anforderungsprofil und ein darauf basierendes Pflichtenheft stellen damit entscheidende Erfolgsfaktoren dar.

Das Pflichtenheft kann in diesem Fall als Checkliste verstanden werden, welches die Rahmenbedingungen und Schlüsselaspekte des jeweiligen Outsourcing-Vorhabens beinhaltet. Mit Hilfe des Pflichtenhefts können also Kriterien herausgearbeitet werden, die eine Vorselektion ermöglichen und auch später bei der Entscheidungsfindung herangezogen werden können.

Nach der Vorselektion ist der nächste mögliche Schritt eine Einholung der Leistungsangebote der in die engere Wahl gekommenen Outsourcing-Anbieter. Abgesehen von dem Leistungsangebot treten an dieser Stelle auch allgemeinere Fragen an den potenziellen IT-Partner in den Vordergrund, wie etwa die Rechtsverhältnisse (Dauer des Bestehens, Rechtsform, Inhaber/Gesellschafter etc.), die wirtschaftlichen Verhältnisse (Bilanzverhältnisse, Umsatz, Mitarbeiteranzahl etc.), die Organisation (erkennbare Organisationsstruktur, Qualitätsmanagement, Zertifizierung etc.) und die Leistungsfähigkeit (Position am Markt, Referenzen, Qualität des Personals, technische Infrastruktur etc). Durch Prüfung dieser Punkte kann ein Unternehmen auf die Bonität und Zuverlässigkeit der IT-Outsourcing-Anbieter schließen (vgl. Köhler-Frost 2002, S. 135f).

Nachdem die Leistungsangebote eingeholt und die allgemeinen Fragen an den IT-Anbieter geklärt wurden, können die Angebote verglichen werden. Dabei spielen sowohl „weiche“ als auch „harte“ Faktoren, wie Preise und Leistungen, eine Rolle. Weiche Faktoren sind schwieriger konkret zu fassen und beruhen z.B. auf den Erfahrungsschatz des Entscheidungsträgers bzw. der Entscheidungsträger.

[7] Zum Thema Anforderungen und Anforderungsmanagement soll vertiefend auf Versteegen/Heßeler (2004) verwiesen werden.

In manchen Situationen können die weichen Faktoren allerdings zur Entscheidung führen, wie etwa im Falle einer Übereinstimmung von Preis- und Leistungsmerkmalen zweier Outsourcing-Dienstleister. Durch einen Bewertungsvergleich kann schließlich die Entscheidung für einen bestimmten Outsourcing-Partner getroffen werden.

Die Aufgabe der Partnersuche und –auswahl wird in der Regel als Projekt[8] verstanden und von einem Projektteam übernommen (vgl. Wißkirchen 1999, S. 206). Die Entscheidung der Partnerwahl wird dadurch auf mehrere Personen aus meistens verschiedenen Fachabteilungen verteilt. Ebenso können externe Berater herangezogen werden.

2.5 Vertragsgestaltung

2.5.1 Letter of Intent

Hat man sich für ein IT-Outsourcing mit geeignetem IT-Dienstleister entschieden, müssen die bei der Partnerwahl in einem Pflichtenheft beschriebenen Anforderungen in einem nächsten Schritt vertraglich festgehalten werden. Ebenso wie die Partnersuche und –auswahl wird auch der Prozess der Vertragsgestaltung in der Regel als Projekt mit dem dazugehörigen Projekt-Management verstanden[9].

Für den Outsourcing-Vertrag gibt es keine gesetzlichen Vorgaben. Dadurch gibt es auch keine verbindlichen Regeln, wie der Vertrag aufgebaut sein soll und welchen Inhalt er haben soll. Durch die Komplexität, die ein Outsourcing-Projekt annehmen kann, ist eine möglichst lückenlose rechtliche Absicherung dennoch wichtig. Ein eindeutiges und kontrollierbares Verhalten der Vertragspartner kann erst dadurch gewährleistet werden. Eine detaillierte Regelung im Vorhinein kann darüber hinaus auf beiden Seiten Klarheit schaffen, welche Vorraussetzungen erfüllt werden müssen, um die Zusammenarbeit zum Erfolg zu führen.

Bevor es zum eigentlichen Vertrag kommt, wird in zahlreichen Praxisfällen zunächst mit dem gewählten Partner ein so genannter Letter of Intent (LoI) unterzeichnet, der später als Grundlage für den eigentlichen Vertrag dient. Bei einem Letter of Intent handelt es sich um Absichtserklärungen, die zwischen Outsourcinggeber und –nehmer erklärt werden In diesem werden bereits die wesentlichen Punkte der Zusammenarbeit zwischen dem Dienstleister und dem Outsourcinggeber festgehalten. Sinn und Zweck des LoI ist es mündliche Vereinbarungen schriftlich festzuhalten. Der LoI stellt in der Regel kein bindendes längerfristiges Angebot dar und ist dementsprechend keine Verpflichtung zum Abschluss eines Rahmenvertrags. Durch das LoI soll dem Vertragspartner signalisiert werden, dass eine ernsthafte Bereitschaft zum Vertragsabschluss vorliegt (vgl. Hodel/Berger/Risi 2004, S.81).

---

[8] Im Gesamtzusammenhang als Teilprojekt verstanden. Vgl. Kapitel 2.6.1 und 2.6.2

[9] Im Gesamtzusammenhang als Teilprojekt verstanden. Vgl. Kapitel 2.5.1 und 2.5.2

Im Bedarfsfall kann einem LoI aber auch eine Rechtswirkung, wie bei einem Vertrag zukommen. Ein Grund für diese Handhabung ist, dass der externe Dienstleister dadurch die Möglichkeit bekommt mit den Vorbereitungen für das Outsourcing zu beginnen, ohne das Risiko einzugehen, dass der Kunde eventuell noch abspringt. Zu den Inhalten eines LoI können beispielsweise zählen (Köhler-Frost 2002, S. 204):

- „Absichtserklärung für Abschluss eines Outsourcing-Vertragswerk,
- Haftungs-, Gewährleistungs- und Fragen der Geheimhaltung,
- Ggf. Aufwandsschätzungen,
- Befristung des Letter of Intent (meist ½ Jahr),
- Exklusivvereinbarungen (der Kunde verhandelt ausschließlich nut mit einem Anbieter),
- Alternativregelungen, wenn Outsourcing-Vertragswerk nicht zustande kommt."

2.5.2 Rahmenvertrag

Die Leistungsverpflichtungen und Rahmenbedingungen werden schließlich im Rahmenvertrag konkretisiert und ausgestaltet. Der LoI dient dabei als Grundlage für den Outsourcing-Vertrag. Beide Seiten, also sowohl Outsourcinggeber als auch Outsourcingnehmer, versuchen dabei ihre Interessen zu wahren. Aus diesem Grund erfolgt die Vorgehensweise bis zum entgültigen Vertragsabschluss in der Regel in mehreren aufeinander folgenden Schritten. Hat der Outsourcinggeber einen Vertragsentwurf ausgearbeitet, wird dieser an den Outsourcingnehmer übersandt. Vom Outsourcingnehmer wird im Gegenzug ein Gegenentwurf ausgearbeitet. Durch eine mündliche Verhandlung zwischen den beiden Seiten, die auf Basis der beiden Vertragsentwürfe stattfindet, kann schließlich eine Einigung erzielt und der Vertrag zum Abschluss gebracht werden (vgl. Zahn/Barth/Hertweck 1998, S.136).

Die Vertragsdauer bei einem Outsourcing-Vorhaben beträgt in der Regel zwischen drei und zehn Jahren. Es handelt sich also um eine längerfristige Bindung. Der Rahmenvertrag sollte deshalb sowohl flexible Variablen (z.B. Einführung neuer Technologien, verschlechterte wirtschaftliche Lage) zulassen, als auch stabile Vorgaben aufweisen. Ein ausgewogenes Verhältnis zu finden, ist wichtig, da zu viele Variablen einerseits und zu starre Vorgaben andererseits den Rahmenvertrag zum Scheitern bringen können (vgl. Hodel/Berger/Risi 2004, S.85).

Zum Inhalt eines Outsourcing-Vertrags gehören u.a. folgende Punkte (Hodel/Berger/Risi 2004, S. 87f):

- „Definition der übergebenen Hauptaufgaben (Details zu Leistungen, Objekte, Verantwortliche und Qualität gehören in die Leistungsverträge bzw. SLAs[10])

[10] Service Level Agreements, vgl. Kapitel 2.5.3

- Vorgehen bei Vertragsverletzungen (mit Unterscheidung leichter / schwerer Vorfälle)
- Management der Zusammenarbeit (Aufführen von Kontakt- und Eskalationsstellen)
- Change und Release Management (Aufzeigen wie das Vorgehen bei Änderungen bzw. Abweichung der definierten Standards, Methoden oder Prozesse ist)
- Projektplan für die Umsetzungsphase (Kosten, Termine, Verantwortlichkeiten, Abnahme, Steuerung etc.).
- Zusicherung des Rechts, geplante Reviews und Revisionen durchzuführen
- Zusicherung der Unterstützung durch den Outsourcingnehmer in Notfällen. Dies kann z.B. bei vorzeitiger Auflösung des Vertrages wichtig sein“

Ein Punkt, der bei der Gestaltung von einem Rahmenvertrag zum IT-Outsourcing ebenfalls berücksichtigt werden kann, ist die Informationssicherheit. Durch das Outsourcing können sich Verantwortlichkeiten im Unternehmen verschieben und ändern. Auch können zusätzliche Schnittstellen entstehen. Unter solchen Vorraussetzungen sollte der Sicherheit von Daten und Informationen auch im Rahmenvertrag eine hohe Aufmerksamkeit gewidmet werden. Auf diese Weise kann ein Rahmenvertrag so gestaltet sein, dass Aufgaben, Kompetenzen und Verantwortlichkeiten für beispielsweise Zutritts- und Zugriffssicherheit, Wartungsfenster und Releasezyklen mitberücksichtigt werden (vgl. Hodel/Berger/Risi 2004, S.86).

Ein Outsourcing-Vertrag[11] kann als Dienstleistungsvertrag aufgefasst werden. (vgl. Bullinger/Rüger/Thiele 1997, S.29) Um auch bei umfangreichen Outsourcing-Projekten, wie bei der Gründung eines Joint-Ventures, rechtlich abgesichert zu sein, kommen zu den Dienstleistungsverträgen meistens noch weitere Verträge, wie Gesellschaftsverträge, Übergabe- und Nutzungsverträge etc. hinzu.

2.5.3 Service Level Agreements

Durch den Rahmenvertrag werden Leistungsverpflichtungen vereinbart. Die Erbringung dieser gilt es abzusichern. Eine Grundlage zur Feststellung, ob der Outsourcing-Vertrag eingehalten wurde, bieten die Service-Level-Agreements (SLAs). Die SLAs können dabei als eigener Absatz innerhalb des Vertrags oder als Anlage zum Vertrag eingebunden sein. Es gibt aber auch die Möglichkeit eines zusätzlichen Vertrags für die SLAs. In diesem Fall ist es als rechtskräftiges Dokument zu verstehen, das auf einem bereits vorhanden Outsourcing-Vertrag basiert.

[11] Für eine vertiefende Vorgehensweise der Vertragsausgestaltung vgl. Zahn/Barth/Hertweck (1998, S.135-165)

Was versteht man nun unter Service-Level-Agreements? „Ein Service-Level-Agreement umfasst die Leistungen, Verantwortlichkeiten, Qualitäten und spezifischen Rahmenbedingungen wie z.B. die Definition von Sanktionsinstrumentarien für den Fall der Unterschreitung der definierten Leistungsstandards“ (Hodel, Berger, Risi 2004, S.88).

SLAs dienen als Messinstrument, um den Grad der Leistungserfüllung zu erkennen. Dazu werden die Serviceleistungen des Outsourcingnehmers in Bezug gesetzt zu den Anforderungen des Auftraggebers. Zielsetzung bei der Beschreibung von SLAs ist es deshalb eine Kosten-, Leistungs- und Qualitätstransparenz zu schaffen. Ein wesentlicher Faktor bei den SLAs sind die vertraglich vereinbarten Strafen bei der Nichteinhaltung der Leistungsabmachungen. SLAs dienen dadurch gleichzeitig als Druckmittel. Zum Inhalt eines SLAs gehören z.B. folgende Punkte (Kaeding 2003, S. 12):

- „Bestimmung der einbezogenen Funktionalitäten (auch der Applikationen)
- Bestimmung der Verfügbarkeit (i.d.R. in %)
- Berechnung der Verfügbarkeit (Formel)
- Festlegen der Ausfallzeiten (Beginn, Ende, Ausnahmen)
- Bestimmung der Dokumentationen
- Bestimmung von Antwort- und Reaktionszeiten
- Festlegen der Vertragsstrafen und Art der Berechnung[12]“

Vor allem zu Beginn einer Outsourcing-Partnerschaft dienen Service-Level-Agreements auch als vertrauensbildende Maßnahme. Sie schaffen eine Basis gemeinsamen Handelns.

2.6 Durchführung eines IT-Outsourcing-Projektes

2.6.1 Phasen des IT-Outsourcing

Für ein besseres Verständnis der komplexen Zusammenhänge aber auch zur Erleichterung der praktischen Durchführung empfiehlt sich für ein Outsourcing-Projekt eine systematisch-methodische Vorgehensweise. Zu diesem Zweck ist es ratsam den Outsourcing-Prozess aufzuspalten und in mehrere überschaubare Phasen aufzugliedern. Abbildung 6 beschreibt die vier Phasen eines Outsourcing-Projektes und deren wichtigste Aktivitäten. Je nach gewählter Outsourcing-Form kann die Abbildung dabei durch zusätzliche Aktivitäten ergänzt werden.

[12] Dieser Punkt wird vom Outsourcinggeber oft vergessen und ist im nachhinein vom Outsourcingnehmer nur schwer nachforderbar.

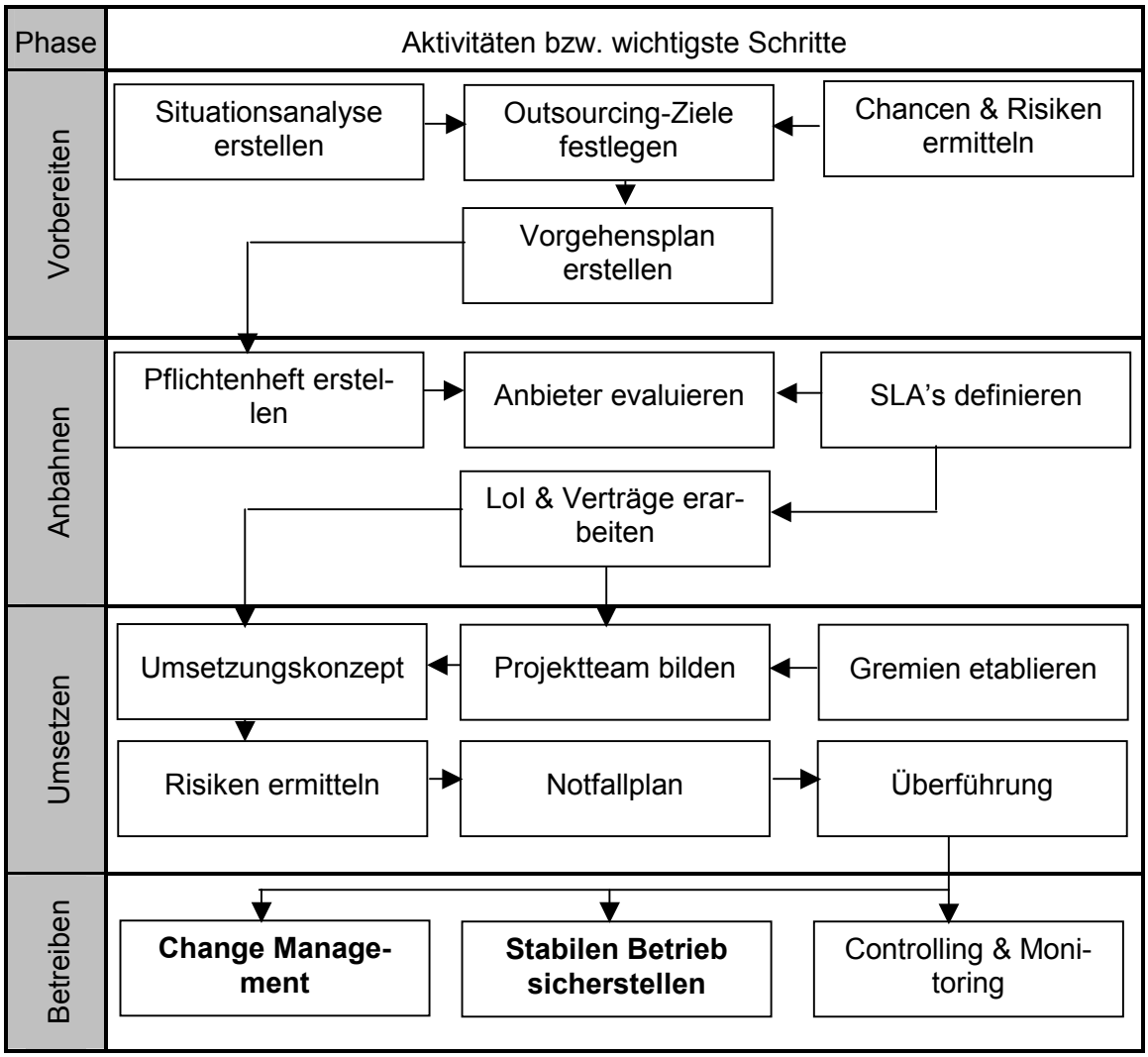


Abbildung 6: Übersicht Phasen und Aktivitäten (Quelle: Hodel, Berger, Risi 2004, S.43)

Die **Vorbereitungsphase** beginnt mit einer Situationsanalyse. Aufgabe der Situationsanalyse ist eine Bestandsaufnahme gegenwärtiger und künftiger Anforderungen des Marktes und die zielbewusst daraus abgeleiteten notwendigen Unternehmensleistungen. Mit Hilfe der Situationsanalyse kann ein Unternehmen erkennen, was es können muss, wenn es sich im Wettbewerb erfolgreich behaupten will.

Hat man durch die Situationsanalyse die Ausgangslage identifiziert, kann man in einem nächsten Schritt die Outsourcing-Ziele festlegen[13]. Steht für ein Unternehmen beispielsweise die Kostenreduktion bei einem Outsourcing der IT im Vordergrund, möchte es eine Reduktion der Betriebskosten und des gebundenen Kapitals erzielen. Steckt ein Unternehmen wiederum in einer Engpass-Situation, weil zu wenig (freie) Kapazitäten zur Verfügung stehen, ist das Zukaufen von Ressourcen der zentrale Gedanke für ein IT-Outsourcing[14]. Für eine optimale Zielereichung sollten die Leistungen des IT-Outsourcing nach den Zielen definiert und abgegrenzt werden.

[13] Möchte man die Make-or-Buy-Entscheidung in das Phasenmodell mit einfügen, so ist sie direkt nach der Festlegung der Outsourcing-Ziele einzusetzen.

[14] Für weitere mögliche Outsourcing-Ziele vgl. Kapitel 2.3

Gemessen an den Nutzenpotenzialen sollten bereits in der Vorbereitungsphase auch die Risiken auf ihre Tragbarkeit untersucht werden. Eine Chancen-Nutzen-Analyse kann dabei weiterhelfen.

Schließlich ist noch die Erstellung eines Vorgehensplans Teil der Vorbereitungsphase. Wichtige Punkte dieses Plans sind die Terminplanung, die Festlegung von Meilensteinen und die Ressourcenplanung. Die Bereitstellung von Ressourcen bedeutet dabei z.B., dass ein Projektleiter bestimmt wird und für die benötigte Zeit freigestellt ist. Ein weiteres Beispiel ist, dass die notwendige personelle und finanzielle Unterstützung für das Outsourcing-Vorhaben zur Verfügung gestellt wird.

Sind die Ressourcen bereitgestellt, kann die **Anbahnungsphase** angegangen werden. Die Anbahnungsphase baut dabei auf den Ergebnissen der Vorbereitungsphase auf. Gegenstand dieser Phase ist die Erstellung eines Pflichtenheftes, die Partnerwahl[15] und die vertraglichen Aktivitäten[16] (LoI, Rahmenvertrag, SLAs), die bereits beschrieben wurden. In der Anbahnungsphase wird somit der Grundstein für die zukünftige Partnerschaft gelegt (vgl. Hodel, Berger, Risi 2004, S.67). Die Ergebnisse dieser Phase dienen wiederum als Grundlage für die nächste Phase, die Umsetzungsphase.

Haben die beiden vorangegangenen Phasen noch der Vorbereitung eines IT-Outsourcing gedient, so soll in dieser Phase die erfolgreiche **Umsetzung** des Outsourcing-Vorhabens erzielt werden. Hauptgegenstand ist also die Überführung und Übernahme der definierten Leistungserbringung durch einen Outsourcing-Provider(vgl. Hodel, Berger, Risi 2004, S.110). Die Überführung gehört zu den anspruchsvollsten und kritischsten Phasen des Outsourcing-Projekts. Für eine erfolgreiche Umsetzung ist deshalb ein systematisches Vorgehen durch Bildung eines Umsetzungskonzepts wichtig. Im Umsetzungskonzept werden dabei die wichtigsten Themen, die im Rahmen der Umsetzung realisiert werden müssen, festgehalten. Dazu gehören beispielweise die Projektorganisation, eine klare Aufgabenverteilung und Ressourcenübernahme.

Für die Umsetzung des Outsourcing-Projekts wird in der Regel ein spezielles Projektteam gebildet, das diese Aufgabe übernimmt. Dieses kann sich sowohl aus Mitgliedern des Outsourcinggebers als auch aus Mitgliedern des zukünftigen Providers zusammensetzen. Weiter werden Gremien gebildet. Durch sie wird sichergestellt, dass stufengerecht kommuniziert wird, da Ansprechpartner von verschiedenen Organisationsebenen des Outsourcinggebers und des Outsourcingnehmers festgelegt werden.

Ein wesentlicher Punkt, der bei der Umsetzungsphase berücksichtigt werden sollte, sind die möglichen Risiken, die bei einem IT-Outsourcing entstehen[17]. Auch ein Notfallplan sollte ermittelt werden. Ergebnis der Umsetzungsphase sollte eine erfolgreiche Überführung des jeweiligen Outsourcing-Gegenstands sein.

---

[15] Vgl. Kapitel 2.4.2

[16] Vgl. Kapitel 2.5

[17] Vgl. Kapitel 3.3

Hat man in der Umsetzungsphase erfolgreich outgesourct, gilt es in der **Betriebsphase** die während des Outsourcing-Projekts erzielten Ergebnisse zu konsolidieren und laufend zu verbessern. Der Übergang zum operativen Betrieb, das Monitoring und Controlling, sowie laufende Anpassungen (Change Management) sind die wesentlichen Aktivitäten dieser Phase (vgl. Hodel, Berger, Risi 2004, S.122).

2.6.2 Projekt Management beim IT-Outsourcing

Bei einem Outsourcing-Vorhaben steht ein Unternehmen vor einer neuartigen und komplexen Aufgabe, die in einem begrenzten Zeitraum erfolgreich abgewickelt werden soll und mit erheblichen Risiken verbunden ist (vgl. Bea/Göbel 1999, S.423). Damit erfüllt es die typischen Merkmale eines Projektes. Die Auslagerung von IT-Leistungen bedeutet für ein Unternehmen also letztendlich die Einrichtung eines komplexen Projektes. Um ein Projekt erfolgreich abwickeln zu können, bedient man sich der Methoden und Werkzeuge des Projekt-Managements. Unter Projekt-Management wird die Planung, Kontrolle, Steuerung und Organisation eines Projektes verstanden. Betrachtungsobjekte des Projekt-Managements[18] sind die Projektziele, Projekttermine, Projektressourcen und Projektkosten, die Projektorganisation und die Projektkultur (vgl. Wallmüller 2004, S. 52).

Zu diesem Zweck wird ein Projektleiter ernannt und ein Projektteam gebildet. Dieses kann sich dabei sowohl aus Mitgliedern des Outsourcinggebers als auch aus Mitgliedern des Outsourcingnehmers zusammensetzen. Nimmt man jede Phase bzw. einzelne Aktivitäten, die im Rahmen des IT-Outsourcing durchgeführt werden müssen, für sich, können Teilprojekte mit einem eigenen Teilprojektleiter und einem Teilprojektteam gebildet werden[19]. Wegen der Fülle an Mitarbeitern, die letztendlich am IT-Outsourcing-Projekt arbeiten können, ist eine klare Aufgaben- und Kompetenzverteilung nötig. Teilprojektleiter und Projektmitarbeiter müssen also Klarheit über ihre Aufgaben, Rollen und Verantwortlichkeiten haben (vgl. Hodel, Berger, Risi 2004, S.113).

Rollen, die bei einem IT-Outsourcing-Projekt unterschieden werden, sind z.B. Projektleitung, Projekt Office, Projektteam, Rechtsabteilung / -beratung, Risk-Manager und Projektsteuerungsgremium. Da IT-Outsourcing-Projekte oft zeitkritisch ablaufen, ist eine Einhaltung von Terminen und Meilensteinen sehr wichtig, vor allem, weil meistens keine oder nur wenige Pufferzeiten miteingeplant werden.

Nehmen Projektmitglieder oder Teilprojektleiter Aufgaben oder Verantwortlichkeiten nicht rechtzeitig wahr, kann deshalb das gesamte Projekt ins Wanken geraten. Die Definition von klaren Vereinbarungen für die wichtigsten Arbeitspakete einschließlich der Zeitvorgaben und eine Überwachung der Ausführungen und Fortschritte ist aus diesem Grund notwendig (vgl. Hodel, Berger, Risi 2004, S.113).

---

[18] Zum Projekt-Management soll vertiefend auf Stöger (2004) verwiesen werden.

[19] Beispiele dafür sind die Partnerwahl und die Vertragsgestaltung, auf die bereits hingewiesen wurde

2.6.3 Wechselwirkung zwischen Projekt- und Risikomanagement

Die Durchführung eines (IT-) Outsourcing-Projekts ist auch bei einer guten Planung mit erheblichen Risiken verbunden, die vom Projekt-Management beachtet werden sollten.

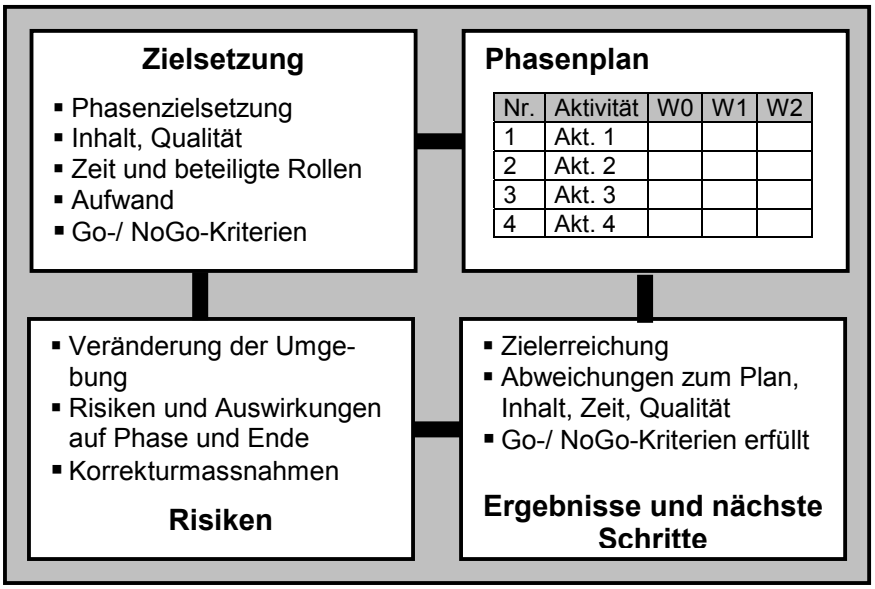


Abbildung 7: Projekt Management (Quelle: Hodel, Berger, Risi 2004, S.142)

Die Nichtbeachtung und Unterschätzung von Risiken wirkt sich in der Regel negativ auf ein Projektergebnis aus (vgl. Stöger 2004, S. 141). Im Extremfall können Risiken sogar den Grund für das Scheitern eines IT-Outsourcing-Projekts bilden. Es gilt deshalb die Risiken zu entschärfen und in einem Rahmen zu halten, der sich tragen lässt. Zu diesem Zweck ist für die Durchführung von IT-Outsourcing-Projekten die Einbeziehung des Risiko-Managements notwendig.

Mit Hilfe des Risiko-Managements können die Risiken erkannt und analysiert sowie Gegenmaßnahmen getroffen werden. Risiko-Management wird heute aus diesem Grund immer häufiger auch als integrierte Teildisziplin des Projekt-Managements verstanden (vgl. Wallmüller 2004, S.52).

Im Folgenden soll zunächst auf die Risiken eingegangen werden, die mit einem IT-Outsourcing-Projekt verbunden sind und anschließend auf das Risiko-Management mit.

3 Risiken beim IT-Outsourcing

3.1 Verpflichtung zur Risikoerfassung durch das KonTraG

Ein Outsourcing der IT kann eine Vielfalt an Nutzenvorteilen für Unternehmen bringen. Doch eröffnen sich durch ein solches Vorhaben nicht nur Chancen. Auch Risiken sind damit verbunden, die zu den Unternehmensrisiken gezählt werden müssen. Schon seit Langem beschäftigt sich die Managementlehre mit den Unternehmensrisiken, ihrer Wahrnehmung, Bewertung und der Ableitung von Handelsoptionen. Die Bedeutung der Risikovorsorge bei Unternehmensrisiken und der damit verbundenen Notwendigkeit der Einführung von Kontrollmechanismen hat auch der deutsche Gesetzgeber erkannt und durch das Gesetz zur Kontrolle und Transparenz seit 1998 für viele Unternehmen verpflichtend gemacht. Durch das KonTraG werden damit präventive Maßnahmen zur Risikoerkennung erzwungen.

Galt das Gesetz zunächst nur für Aktiengesellschaften, werden heute durch weitere Gesetzgebungen auch GmbHs davon erfasst (vgl. http://www.risknet.de/Data/risknews07_2000.pdf).

Des weiteren gilt für andere Unternehmensrechtsformen, das zwei der nachfolgenden drei Kriterien erfüllt sein müssen (vgl. Versteegen 2003, S. 5):

- die Bilanzsumme beträgt über 3,44 Mio. Euro,
- der Umsatz beträgt mehr als 6,87 Mio. Euro
- das Unternehmen hat mehr als 50 Mitarbeiter.

Das KonTraG verpflichtet die davon betroffenen Unternehmen, ein Überwachungssystem einzurichten, dass Entwicklungen frühzeitig erkennt, die den Fortbestand der Gesellschaft gefährden.

§ 91 Absatz 2 AktG lautet deshalb: „Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden."

Durch einen unabhängigen Wirtschaftsprüfer wird die Umsetzung des Risiko-Management-Systems nach den Richtlinien des KonTraGs überprüft. Für die Einhaltung haften deshalb die Geschäftsleitung, der Aufsichtsrat aber auch der Wirtschaftsprüfer. Durch das KonTraG wird keine genaue Beschreibung des Risiko-Managements festgesetzt, so dass keine einheitliche Regelung zu finden ist und die Ausgestaltung den Unternehmen überlassen bleibt. Der Gesetzgeber fordert die Unternehmen über das KonTraG lediglich auf, im Rahmen eines Risikofrüherkennungssystems alle wesentlichen Unternehmensrisiken frühzeitig zu erfassen.

Nach herrschender Meinung stellt das gesetzlich geforderte Risikofrüherkennungssystem jedoch ein integriertes Risiko-Management-System dar, das alle Unternehmensbereiche berücksichtigt. Das schließt komplexe Projeke, wie das IT-Outsourcing, mit ein (vgl. Gaulke 2002, S. 17f).

Dementsprechend sind alle Unternehmensbereiche nach Risiken zu untersuchen, was komplexe Projekte wie ein Outsourcing der IT mit einschließt. Auch die Risiken, die bei einem IT-Outsourcing-Projekt entstehen, gehören damit dazu. Im Folgenden soll deshalb zunächst ein allgemeiner Überblick über mögliche Risiken des IT-Outsourcings gegeben werden, um dann auf das Risiko-Management einzugehen.

3.2 Begriffsklärung und Überblick über die Risiken beim IT-Outsourcing

Zunächst stellt sich die Frage, was eigentlich unter dem Begriff Risiko zu verstehen ist. An dieser Stelle soll deshalb der Risikobegriff erläutert werden und ein Überblick über die Risiken des IT-Outsourcings gegeben werden. Auf diese wird in den darauf folgenden Kapiteln ausführlich eingegangen.

Das Wort Risiko hat seinen Ursprung im frühitalienischen Wort „risicare“, das übersetzt „etwas wagen“ bedeutet. Obwohl sich zahlreiche Veröffentlichungen mit der Risikoproblematik wirtschaftlichen Handelns beschäftigen, gibt es trotz der Fülle keine einheitliche und allgemeingültige Definition des Risikobegriffs.

Zwei grundlegende Orientierungen bei der Bestimmung des Begriffs Risiko sind jedoch erkennbar. Zum einen gibt es die ursachenbezogenen Begriffsbestimmungen. Diese sind durch die Verknüpfung betrieblicher Entscheidungssituationen mit dem Risikobegriff gekennzeichnet. Im Mittelpunkt steht dabei der unvollkommene Informationsstand bei einer Entscheidungssituation (vgl. Junginger 1999, S. 9).

Zum anderen gibt es die wirkungsbezogenen Begriffsbestimmungen. Kernpunkt dieser sind die negativen Konsequenzen als Folge betrieblicher (Fehl-)Entscheidungen (vgl. Junginger 1999, S. 10). Letztendlich werden also bei den beiden Orientierungen zur Begriffbestimmung die Aspekte der Unsicherheit über ein Ereignis und der Ungewissheit über die Auswirkungen eines Ereignisses berücksichtigt.

Eine Definition, die beide Aspekte berücksichtigt, beschreibt das Risiko als ein *„Ereignis, von dem nicht sicher bekannt ist, ob es eintreten und/oder in welcher genauen Höhe es einen Schaden verursachen wird“* (Gaulke 2002, S. 10).

Eine weitere Definition betrachtet den Risikobegriff, wie folgt (Kirchner 2002, S. 16):

> *„Risiko ist die Möglichkeit des Nicht-Erreichens einer Zielsetzung bzw. Strategieformulierung, weil Handlungen oder Ereignisse innerhalb oder außerhalb des Unternehmens störend auf die materiellen, immateriellen oder personellen Erfolgsfaktoren des Unternehmens einwirken und so die Möglichkeit der Wahrnehmung von zukünftigen Entwicklungschancen aufgrund eines Informationsdefizits über die*

kausalen Ursache-Wirkungs-Beziehungen der genannten Faktoren und die wirtschaftliche Lage beeinflussen.“

Auch ein Outsourcing der IT ist mit Risiken verbunden. Grundsätzlich lassen sich die Risiken, die durch ein IT-Outsourcing-Projekt entstehen, chronologisch in ihrer Entstehung unterteilen. Zunächst entstehen Risiken während der Projektphasen. Darunter ist der Outsourcing-Prozess vom Zeitpunkt der Planung bis zur Überführung der IT an einen IT-Dienstleister zu verstehen. Ist die IT überführt, können durch das IT-Outsourcing Risiken auch in der Betriebsphase entstehen. Die Betriebsphase beginnt dabei also mit der Überführung und der anschließenden Rückkehr in den nun veränderten Betriebsablauf. Abbildung 8 systematisiert die Risikokategorien, die in diesen beiden Phasen zu berücksichtigen sind.

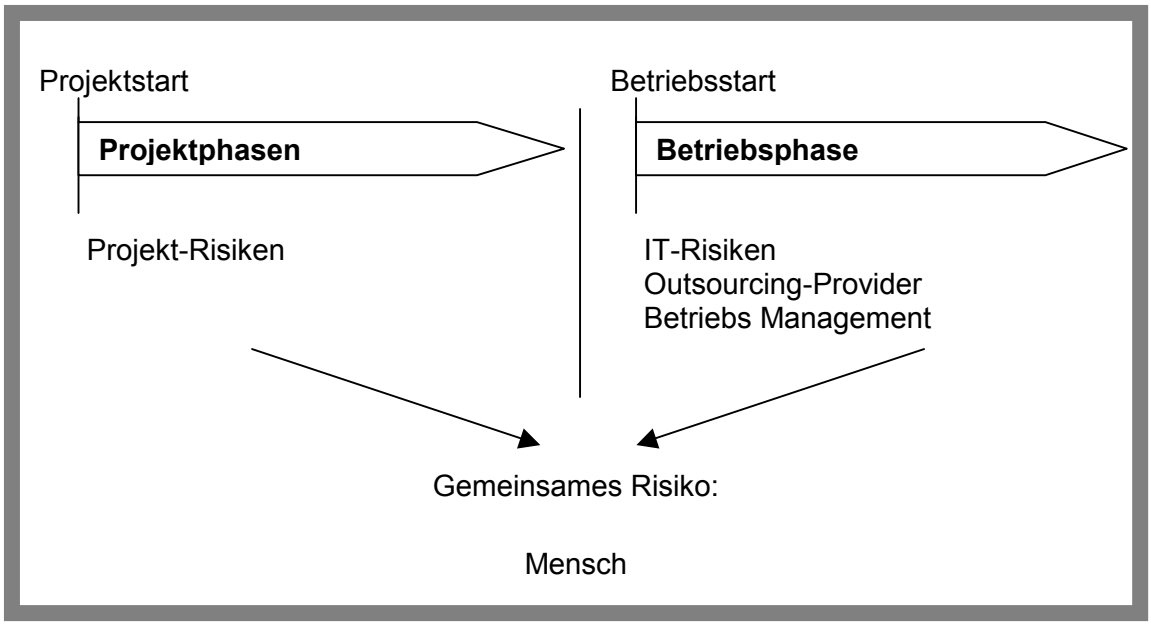


Abbildung 8.: Risikokategorien bei einem IT-Outsourcing-Projekt (Quelle: Eigene Darstellung)

Hinter den in der Abbildung dargestellten Risikokategorien verbergen sich eine Fülle von Risiken, auf die nun eingegangen wird. Dabei soll lediglich ein allgemeiner Überblick vermittelt und kein Anspruch auf Vollständigkeit erhoben werden, da jedes IT-Outsourcing-Projekt verschieden ist und dementsprechend auch in den Risiken differieren kann.

3.3 Risiken während der Projektphasen

3.3.1 Projektrisiken

Dem zeitlichen Verlauf entsprechend soll zunächst auf die Risiken, die während der Projektphasen entstehen können, eingegangen werden.

Ein IT-Outsourcing-Projekt ist, wie jedes andere Projekt auch, allgemeinen Risiken ausgesetzt. Dazu gehören beispielsweise die Verfügbarkeit von Ressourcen, die Plausibilität der Meilensteine, die Verfügbarkeit der Werkzeuge, die Einhaltung von Terminen und ein Fehlendes oder unzureichendes Test- und Freigabeverfahren. Diese Risiken[20] sind allgemeine Risiken, die auch für andere Projekten gelten. Neben solchen allgemeinen Risiken des Projekt Managements gibt es aber auch Projektrisiken, die nur bei IT-Outsourcing-Projekten auftreten. Orientiert man sich an den Phasen des IT-Outsourcings lassen sich z.B. folgende Risken benennen:

- Definition der Outsourcing-Ziele

  Durch die Formulierung von Zielen wird festgelegt, welchen Nutzen man von einem IT-Outsourcing erwartet. Werden die Ziele unklar definiert, kann dadurch u. U. der Nutzen nicht in vollem Umfang erreicht werden. Ein weiterer Risikofaktor bei der Definition von Outsourcing-Zielen ist die Realisierbarkeit derselben.

- Definition der Outsourcing-Leistungen

  Bei der Festlegung des Outsourcing-Gegenstands wird entschieden, welche Leistung bzw. Leistungen nicht mehr intern, sondern von einem externen IT-Dienstleister erbracht werden. Nicht zuletzt durch unpräzise Formulierungen entstehen besondere Risiken. Obwohl die auszulagernde Leistung bezüglich Art, Umfang und Inhalt bekannt sein müsste, zumal sie bislang intern erbracht wurde, gibt es für die zu erbringende Leistung Interpretationsspielräume (vgl. Zahn/Barth/Hertweck 1998, S.19). Zwei Gründe sind dafür zu nennen. Der eine Grund liegt in vielen Fällen bei der Schwierigkeit Leistungen genau in Worte zu fassen, da auch Ausnahmen und Unregelmäßigkeiten zu beschreiben sind. Der zweite Grund für Interpretationsspielräume beruht auf überzogene oder häufig wechselnde Erwartungen. Leistungen müssen sich mit zunehmender Dauer der Partnerschaft den gegebenen Erfordernissen anpassen. Vertraglich kann so ein Sachverhalt im Vorfeld nicht festgelegt werden (vgl. Zahn/Barth/Hertweck 1998, S.19).

- Partnerwahl

  Die Wahl des IT-Dienstleisters wird in der Vorbereitungsphase getroffen und stellt damit zunächst einen Risikofaktor während der Projektphasen dar. Oft lassen Unternehmen nämlich nicht die nötige Sorgfalt bei der Partnerwahl walten. Durch ein mangelhaft ausgeführtes Auswahlverfahren erhöhen sich die Risiken eines Fehlgriffs. Die Nachwirkungen einer falschen Entscheidung bei der Partnerwahl sind dabei in der Regel erst in der Betriebsphase zu spüren, wenn es um die tatsächliche Leistungserbringung geht.

- Unzulängliche vertragliche Regelungen mit einem externen Dienstleister

  Auch das Risiko einer unzulänglichen Vertragsgestaltung gehört zunächst zu den Risiken, die während der Projektphasen beachtet werden müssen.

[20] Zu den Projekt-Risiken soll vertiefend auf Gaulke (2002) verwiesen werden.

Wie bei der Partnerwahl sind die Nachwirkungen dabei vor allem in der Betriebsphase zu bemerken, wenn durch ungenaue Regelungen die Outsourcing-Partnerschaft leidet. Vor allem für den Outsourcinggeber stellt der Vertrag ein wichtiges Kontrollinstrument dar. Es ist die Basis der Leistungserbringung durch den Provider. Eine unklare vertragliche Regelung mit dem IT-Dienstleister in der Vorbereitungsphase stellt damit ein großes Risiko dar. Aber auch eine Überreglementierung des Rahmenvertrags und der SLAs kann zu Problemen führen und stellt ebenso einen Risikofaktor dar (vgl. Hodel/Berger/Risi 2004, S.198).

- Mangelhafte IT-Sicherheit in der Übergangsphase

  Die Übergangsphase der IT vom Outsourcinggeber hin zum Outsourcingnehmer wird oftmals von Termin- und Leistungsvorgaben begleitet. Durch hohe Arbeitsbelastungen und Zeitdruck werden oftmals Aspekte, wie die Entwicklung und Einführung eines IT-Sicherheitskonzeptes, ausgelassen. Die Folge davon ist, dass die Überführung der IT unter geringen Sicherheitsstandards erfolgt.[21] Datensicherheit und Datenschutz können dadurch nicht in vollem Umfang gewährleistet werden (vgl. http://www.bsi.de/gshb/deutsch/menue.htm).

- Unzureichendes Notfallvorsorgekonzept

  Eine unzureichende Notfallvorsorge kann beim Outsourcing schnell gravierende Folgen haben. Im Falle eines Teil- oder Totalausfalls der IT-Systeme kann es dadurch zu langen Ausfallzeiten kommen, die mit entsprechenden Folgen für die Produktivität bzw. Dienstleistung des Auftraggebers verbunden sind (vgl. http://www.bsi.de/gshb/deutsch/menue.htm).

- Unterschätzung der Outsourcing-Kosten

  Bei der Planung der Kosten kann es durch fehlerhafte kostenrechnerische Verfahren zu einer Unterschätzung der Outsourcing-Kosten kommen. Durch ein Outsourcing der IT entstehen grundsätzlich Transaktionskosten in Form von Koordinations-, Kommunikations- und Kontrollkosten. Oft müssen beispielweise aufwendige Kommunikationseinrichtungen installiert werden. Vor allem bei internationalen Outsourcing-Vorhaben treten Probleme solcher Art verstärkt auf (vgl. Zahn/Barth/Hertweck 1998, S.17).

3.3.2 Mensch

Ein Risikofaktor, sowohl in den Projektphasen als auch in der Betriebsphase, ist der Mensch. Ein Outsourcing der IT bringt zunächst Veränderungen mit sich und das schafft in vielen Fällen Verunsicherung. Vor allem bei den direkt betroffenen Mitarbeitern schürt die Ankündigung eines Outsourcing-Vorhabens zunächst Ängste (z.B. vor Verlust des Arbeitsplatzes). Aber auch in anderen Bereichen, neben den direkt betrof-

[21] Gründe für das oftmalige Fehlen von IT-Sicherheitskonzepten ist auch in der Einstellung der Mitarbeiter zu suchen. Viele arbeiten unter dem Motto “Hauptsache es läuft“

fenen, verursacht die Ankündigung eines solchen Vorhabens zunächst Verunsicherung. Das gilt vor allem für diejenigen Mitarbeiter, die eng mit den Betroffenen zusammenarbeiten (vgl. Hodel/Berger/Risi 2004, S. 117).

Durch diese allgemeine Verunsicherung der Mitarbeiter entstehen weitere Risikofaktoren für das Outsourcing-Projekt. Dazu gehören:

- Störung des Betriebsklimas durch ein Outsourcing-Vorhaben
- Widerstand im auslagernden Unternehmen
- Innere Kündigung, und einem dadurch resultierenden Dienst nach Vorschrift
- Mitarbeiter akzeptieren neue Situation nicht
- Manager haben Mühe mit neuer Position

3.4 Risiken in der Betriebsphase

3.4.1 Outsourcing-Provider

Wie bereits bei der Erläuterung der Risiken in den Projektphasen erwähnt wurde, stellt die Auswahl des IT-Dienstleisters ein Risiko dar. Entscheidet man sich in den Projektphasen für den falschen IT-Dienstleister hat man als Unternehmen vor allem in der Betriebsphase darunter zu leiden. Aber auch bei einer guten Partnerwahl, gibt es allgemeine Risiken, die durch die Zusammenarbeit mit einem IT-Dienstleister entstehen.

Folgende Risiken verbergen sich deshalb unter anderem hinter der Überschrift IT-Dienstleister:

- Starke, langfristige Abhängigkeit

  Nicht jede Art der Leistungserbringung führt zur selben Abhängigkeit vom IT-Dienstleister. Bei einfacher und leichter Imitierbarkeit der Leistung ist keine zu große Abhängigkeit zu befürchten. Ein Grund dafür ist der große Konkurrenzdruck auf dem IT-Dienstleister-Markt, der den Wechsel des IT-Dienstleisters erleichtert (vgl. Zahn/Barth/Hertweck 1998, S.16).

  Bei komplexer Leistungserbringung liegt die Problemstellung anders vor. In solchen Fällen ist meistens, zumindest kurzfristig, die Entscheidung zur Auslagerung solcher Leistungen nicht reversibel (vgl. Zahn/Barth/Hertweck 1998, S.16).

  Das Risiko der Abhängigkeit wird vom IT-Dienstleister geteilt. Viele IT-Dienstleister konzentrieren sich auf einige wenige Kunden. Dadurch laufen sie Gefahr zu starken Preissenkungen gezwungen zu werden oder eine wichtige Umsatzquelle zu verlieren (vgl. Zahn/Barth/Hertweck 1998, S.16).

- Unterschiedliche Unternehmenskulturen

  Jedes Unternehmen hat seine eigene Unternehmenskultur. Haben Outsourcinggeber und -nehmer zu unterschiedliche Kulturen kann das zu einem Risiko im Hinblick

auf die Zusammenarbeit führen. Unterschiedliche Denkansätze, Verhaltensweisen, Unternehmenssprachen, Normen und Werte können zu Missverständnissen führen. Auch besteht die Gefahr, dass andere Arbeitsstile gegenseitig nicht akzeptiert werden (vgl. Hodel/Berger/Risi 2004, S. 199).

- Qualität der Leistungserbringung

  Nicht jeder IT-Dienstleister hat einen großen Erfahrungsschatz vorzuweisen. Auch gibt es qualitative Unterschiede bei der Leistungserbringung. Dadurch entsteht das Risiko, dass Zusagen hinsichtlich Qualität nicht eingehalten werden können (vgl. Hodel/Berger/Risi 2004, S. 199). Bei einer Zusammenarbeit mit einem externen Dienstleister sind deshalb aufwendige Steuerungs- und Kontrollmechanismen erforderlich[22].

- Kündigung des Vertrags durch den Outsourcingnehmer

  Auch eine plötzliche Kündigung durch den Outsourcingnehmer kann für den Outsourcinggeber ein Risiko darstellen. In einem solchen Fall kann der Zeitpunkt der Vertragskündigung vom auslagernden Unternehmen nicht autonom bestimmt werden. Das Risiko stellt sich für den Outsourcinggeber, wie folgt, dar.

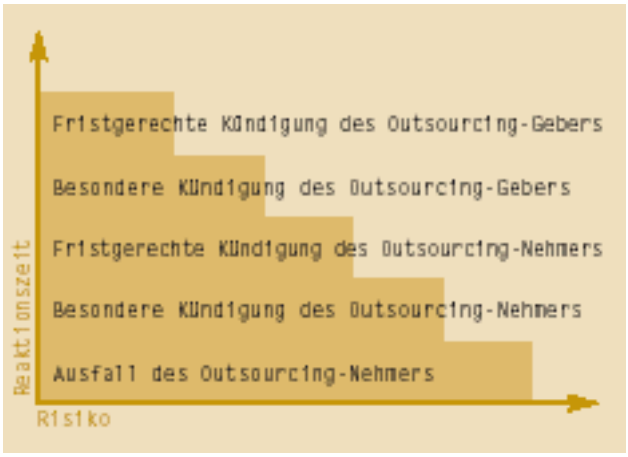


Abbildung 9: Risikodarstellung aus Sicht des Outsourcinggebers (Quelle: Gammelin 2004, S. 30)

Wie die Abbildung verdeutlicht, wird die Reaktionszeit, die dem Outsourcinggeber bleibt, sehr kurz, wenn der Provider ausfällt, wohingegen bei einer fristgerechten eigenen Kündigung der größte Spielraum zu erwarten ist.

- Weitergabe von Daten an Dritte durch den Outsourcing-Dienstleister

  Vor allem große IT-Dienstleister haben in der Regel mehrere Kunden. Dadurch besteht die Möglichkeit, dass sich auch Wettbewerber unter den Kunden befinden. Wurde keine strikte Trennung der Auftragsbearbeitung von verschiedenen Kunden vorgenommen, kann es zu Interessenskonflikten kommen, wenn ein IT-Dienstleister

parallel die Aufträge zweier Konkurrenzorganisationen abdeckt. In solchen Fällen besteht das Risiko, dass Mitarbeiter oder Unterauftragnehmer des Dienstleiters absichtlich oder durch Fehler beispielsweise Arbeitsergebnisse oder solche aus der Projektbearbeitung dem Mitbewerber verfügbar machen. Auch wenn einzelne Personen oder der IT-Dienstleister als ganzes später juristisch zur Verantwortung gezogen werden können, ist ein so entstandener Schaden in der Regel nicht mehr vollständig behebbar (vgl. http://www.bsi.de/gshb/deutsch/menue.htm).

3.4.2 IT-Risiken

Die IT eines Unternehmens ist selbst ein Risikobereich. Allgemein lassen sich die Bedrohungen der IT-Risiken in drei große Bereiche einteilen. Für ein besseres Verständnis soll hier auf diese kurz eingegangen werden.

Der erste Bereich ist der Verlust der Verfügbarkeit. Unter der Verfügbarkeit wird die Eigenschaft eines IT-Systems verstanden, innerhalb eines definierten Zeitraums bestimmte Dienstleistungen in zugesicherter Form und Qualität zu erbringen. Der zweite Risikobereich ist der Verlust der Vertraulichkeit. Dabei wird unter Vertraulichkeit die Eigenschaft eines IT-Systems verstanden, vertrauliche Daten und Informationen nur berechtigten Anwendern und Programmen zugänglich zu machen. Der Verlust der Integrität stellt schließlich den dritten Bereich der IT-Risiken dar. Unter Integrität eines IT-Systems ist dabei die Eigenschaft zu verstehen, dass bei den innerhalb des IT-Systems enthaltenen Daten nur erlaubte und beabsichtigte Veränderungen zugelassen werden.
(vgl.http://www.risikomanagement-in-it-projekten.de/IT-Risiken/IT-Risikodimensionen/it-risikodimensionen.html)

Überträgt man diese Grundbedrohungen auf die IT-Risiken, die durch ein IT-Outsourcing entstehen, lässt sich feststellen, dass vor allem in Bezug auf die Verfügbarkeit der IT und vertraulicher Informationen IT-Risiken entstehen. Dabei ist festzuhalten, dass IT-Risiken nicht nur durch Fehler des IT-Dienstleisters entstehen, sondern auch durch eine schlechte IT-Sicherheit im auszulagernden Unternehmen. Nachfolgende IT-Risiken können u.a. bei einem IT-Outsourcing auftreten:

- Ausfall der Systeme des Outsourcingnehmers

  Fallen die IT-Systeme des Dienstleisters ganz oder teilweise aus, ist auch der Outsourcinggeber davon betroffen. Die Datenverarbeitung kann, auch wenn nur einige Systeme oder Applikationen vom Ausfall betroffen sind, inkonsistent und fehlerhaft werden (vgl. http://www.bsi.de/gshb/deutsch/menue.htm).

  Außerdem ist zu berücksichtigen, dass ein IT-Ausfall zu erheblichen finanziellen Einbußen für den Outsourcinggeber führen kann.

[22] Vgl. Kapitel 2.5

- Schlechte oder fehlende Authentikation

  Zur Authentikation von Benutzern oder Komponenten, sowie zur Bestimmung des Datenursprungs, können Authentikationsmechanismen eingesetzt werden. Sind diese Mechanismen beim Outsourcinggeber schlecht oder fehlerhaft, kann es dazu kommen (vgl. http://www.bsi.de/gshb/deutsch/menue.htm), dass

  - Unbefugte Zutritt auf die IT-Systeme oder Daten bekommen,
  - der Verursacher von Problemen nicht identifiziert werden kann und
  - eine Bestimmung der Herkunft von Daten nicht erfolgen kann.

  Sicherheitslücken entstehen dabei, wenn z.B. bei der Benutzerauthentikation leicht zu erratende Passwörter gewählt werden oder diese in regelmäßigen Abständen geändert werden. Durch schlechte oder fehlende Authentikation kann es also zu einer Gefahr für die Vertraulichkeit und Integrität von IT-Systemen kommen (vgl. http://www.bsi.de/gshb/deutsch/menue.htm).

- Unzureichende Zutrittskontrollen

  Eng verbunden mit der Authentikation ist die Vergabe von Zugriffsrechten. Nicht alle Mitarbeiter sollten dieselben Zugriffsrechte besitzen. Eine Einführung von Zutrittskontrollen ist deshalb wichtig, vor allem, wenn externe Dienstleister auf unternehmensinterne IT-Systeme Zugriff haben. Schon unternehmensintern führt die schlechte Vergabe von Zugriffsrechten schnell zu Sicherheitslücken. Im Falle eines IT-Outsourcings wirkt sich das umso gravierender aus, da dadurch dem externen IT-Dienstleister u.U. Zugriff auf schützenswerte Informationen und Daten ermöglicht wird (vgl. http://www.bsi.de/gshb/deutsch/menue.htm).

3.4.3 Betriebs Management

Ein Outsourcing der IT hat je nach gewählter Form und Umfang auch Auswirkungen auf den laufenden Betrieb. Zu den Risiken der Betriebsphase gehören u.a.:

- Verlust von Know-how

  Das Risiko des Verlustes von Know-how ist besonders gravierend, wenn Kernleistungen oder vermeintliche Unterstützungs- bzw. Randaktivitäten mit unerkannten Kernkompetenzen nach außen vergeben worden sind (vgl. Zahn/Barth/Hertweck 1998, S. 16). Der unkontrollierte Wissensabfluss stellt damit einen kritischen Risikofaktor dar, vor allem da eigene Stärken aus der Hand gegeben werden könnten. Dabei ist zu beachten, dass durch das Outsourcing in der Regel die Kompetenzen eines Unternehmens in diesem Bereich erlöschen. Möchte das Unternehmen später die ausgelagerte IT in das Unternehmen zurückholen, stellt dieser Vorgang durch das Fehlen von Know-how ein Problem dar (vgl. Zahn/Barth/Hertweck 1998, S. 16f).

- Kosten

  Auf den ersten Blick ist ein IT-Outsourcing ein guter Weg zur schnellen Kostensenkung. Kosteneinsparungen ergeben sich jedoch nicht zwangsläufig. In manchen Fällen werden Unternehmen nach dem Auslagern in der Betriebsphase sogar mit mehr Gesamtkosten konfrontiert (vgl. Zahn/Barth/Hertweck 1998, S. 17). Mangelnde Fixkostenreduktion, Umstellungskosten und höhere Transaktionskosten sind Beispiele dafür.

- Verlust von Entscheidungsspielräumen

  Die Übergabe von IT an einen externen Dritten kann einen tiefen Einschnitt in die Unternehmensautonomie mit sich bringen, vor allem, wenn die ausgelagerten Leistungen für das Unternehmen wichtig sind. Der Outsourcinggeber kann Entscheidungen nur noch unter Berücksichtigung des Outsourcingnehmers treffen. Eine rasche Entscheidungsfindung kann so durch langwierige Abstimmungsprozesse zur Konsensfindung behindert werden.

3.4.4 Mensch

Neben den beschriebenen Risiken des IT-Dienstleisters, der IT-Risiken und der Risiken für den laufenden Betrieb können auch in der Betriebsphase Risiken durch menschliches Fehlverhalten entstehen. Beispielhaft sollen hier Möglichkeiten für menschliches Fehlverhalten aufgezeigt werden (http://www.bsi.de/gshb/deutsch/menue.htm):

- „Mitarbeiter holen versehentlich Ausdrucke mit personenbezogenen Daten nicht am Netzdrucker ab.
- Es werden Datenträger versandt, ohne dass die vorher darauf gespeicherten Daten physikalisch gelöscht wurden.
- Dokumente werden auf einem Webserver veröffentlicht, ohne dass geprüft wurde, ob diese tatsächlich zur Veröffentlichung vorgesehen und freigegeben waren.
- Aufgrund von fehlerhaft administrierten Zugriffsrechten vermag ein Mitarbeiter Daten zu ändern, ohne die Brisanz dieser Integritätsverletzung einschätzen zu können.
- Neue Software wird mit nicht anonymisierten Daten getestet. Nicht befugte Mitarbeiter erhalten somit Einblick in geschützte Dateien bzw. vertrauliche Informationen. Möglicherweise erlangen überdies auch Dritte Kenntnis von diesen Informationen, weil die Entsorgung von "Testausdrucken" nicht entsprechend geregelt ist.
- Beim Ausbau, Verleih, Einsendung zur Reparatur oder Ausmusterung von Festplatten können Daten auf zum Teil intakten Dateisystemen in unbefugte Hände gelangen.“

4 Risikomanagement

Die Systematisierung der Risiken bei einem IT-Outsourcing hat gezeigt, dass die Zahl an potenziellen Risiken bei einem solchen Vorhaben sehr groß ist. Dabei wurde nur ein allgemeiner Überblick gegeben. Bei der praktischen Durchführung ist jedes IT-Outsourcing-Projekt verschieden und weißt individuelle Risiken auf, die berücksichtigt werden sollten. Die Fülle an Risiken zeigt die Notwendigkeit von Lösungsvorschlägen. Die Nichtbeachtung von einer solchen Vielzahl von Risiken stellt praktisch selbst eine Gefahr oder anders ausgedrückt ein Risiko dar. Ein Instrument zum Umgang mit Risiken stellt das Risiko-Management dar. Die Begleitung eines IT-Outsourcing-Projekts durch das Risiko-Management wird aus diesem Grund zunehmend als Erfolgsfaktor betrachtet, der maßgeblich für eine erfolgreiche Realisierung des Outsourcing-Vorhabens beiträgt. In den nachfolgenden Kapiteln soll zunächst auf Grundlagen des Risiko-Managements bei Projekten und speziell auf die Rolle des IT-Risiko-Managements eingegangen werden. Wie das Risiko-Management bei einem IT-Outsourcing-Projekt angewendet werden kann, soll im Anschluss in Form eines Leitfadens erläutert werden.

4.1 Begriffsklärung

Bevor nun auf die Methoden des Risiko-Managements eingegangen wird, soll zunächst geklärt werden, was unter dem Begriff des „Risiko-Managements“ zu verstehen ist.

Ähnlich wie beim Risikobegriff, gibt es in der Literatur auch zum Begriff des "Risiko-Managements" eine Vielzahl an Definitionen. Prinzipiell ist Risiko-Management eine systematische Vorgehensweise im Umgang mit Risiken. Für ein besseres Verständnis helfen allgemeine Definitionen. In einer allgemeineren Definition werden unter Risiko-Management "alle erforderlichen Aufgaben und Maßnahmen zur Risikobekämpfung“ (Gaulke 2002, S. 11) verstanden.

An dieser Stelle soll aber auch die tiefergehende Definition von Wallmüller herangezogen werden (Walmüller 2004, S. 10):

> *"Risikomanagement ist ein systematischer Prozess zur Identifikation, Analyse und Kontrolle im Sinne von Überwachung und Steuerung von Risiken in Projekten oder Organisationen."*

Aufgabe des Risiko-Managements ist es also, die wesentlichen Risiken, die den Unternehmenserfolg oder -bestand gefährden, frühzeitig zu erkennen und Gegenmaßnahmen zu treffen. Risiken können dabei in sehr zahlreichen Erscheinungsformen auftreten. Die Systematisierung der Risiken in verschiedene Arten, kann deshalb für eine effiziente Identifikation von Risiken sehr hilfreich sein.

Zu einer weiteren Systematisierung der Risikoarten wird häufig zwischen Einzelrisiko und Gesamtrisiko, sowie zwischen reinen und spekulativen Risiken unterschieden. Aus betriebswirtschaftlicher Sicht kann die Risikoverteilung einer einzelnen Entscheidung als Einzelrisiko bezeichnet werden. Durch die Berücksichtigung der Ergebnisse aller Einzelentscheidungen kann das Aggregat der Einzelrisiken als Gesamtrisiko identifiziert werden (vgl. Krcmar 2003, S. 359). In der wirtschaftlichen Gesamtbetrachtung ist dabei davon auszugehen, dass sich positive und negative Ergebnisse ausgleichen. Das Gesamtrisiko darf deshalb nicht als einfache Summe der Einzelrisiken verstanden werden. Auch können Einzelrisiken eine korrelative Wirkung haben, die auf das Gesamtrisiko nachhaltige Wirkungen haben (vgl. Krcmar 2003, S. 359).

Die Unterscheidung von reinen und spekulativen Risiken andererseits systematisiert die möglichen Ergebnisabweichungen von einem Plan. Von reinen Risiken spricht man dabei, wenn ausschließlich negative Ergebnisabweichungen möglich sind. Spekulative Risiken sind im Gegenzug solche, die sowohl positive als auch negative Abweichungen von einer vordefinierten Zielerreichung zulassen (vgl. Krcmar 2003, S. 359).

Wie auch diese Systematisierung der Risiken in Risikoarten verdeutlicht, bietet das Risiko-Management prinzipiell die Möglichkeit eines systematischen Umgangs mit Risiken. Dabei ist der Grundgedanke des Risiko-Managements vorausschauend zu handeln. Versteegen hat diesen Sachverhalt zu folgender Regel geformt: „Die Behebung eines bereits eingetretenen Risikos ist um ein vielfaches teuerer als das vorausschauende Risikomanagement“ (Versteegen 2003, S.1)

Ein Risiko sollte also – soweit möglich – im Vorfeld erkannt und auch im Vorfeld eliminiert werden. Es gilt also die Eintrittswahrscheinlichkeit von Risiken zu minimieren und die Auswirkungen, falls ein Eintreten unumgänglich ist oder nicht verhindert werden konnte, in einem akzeptablen Rahmen zu halten.

4.2 Risikokultur

Das Risiko-Management berührt in seiner Tätigkeit diverse Verantwortungsbereiche und Zuständigkeiten. Interessen- und Zielkonflikte sind deshalb häufig unumgänglich. Der Erfolg eines Risiko-Managements ist allerdings von der Kommunikation und Information aller beteiligten Personen in einem Projektteam abhängig (vgl. Romeike/Finke 2003, S. 148). Zu einem effizienten Risiko-Management führt nämlich in der Regel erst die Zusammenführung verschiedener Informationen. Der Erfolg des Risiko-Managements wird also in besonderem Maße davon beeinflusst, wie es von den beteiligten Personen gelebt wird. In einem für Risiken sensibilisierten Unternehmen kann es also besser realisiert werden. Ein wichtiger Faktor zur erfolgreichen Umsetzung des Risiko-Managements ist deshalb eine gelebte Risikokultur (vgl. Romeike/Finke 2003, S. 148).

Sie bildet das Fundament der einzelnen Risikomaßnahmen, die im Rahmen des Risiko-Managements getroffen werden. Eine Risikokultur beinhaltet die Bereitschaft zur Wahrnehmung von Risiken, die Sensibilisierung der Mitarbeiter und die Kommunikation der Risiken. Effizient ist eine Risikokultur dann, wenn erkannte Risiken als Chance für ein frühzeitiges Ergreifen von geeigneten Gegenmaßnahmen betrachtet wird. Eine Risikokultur ist geprägt durch ein gemeinsames Werte- und Normengerüst der Mitarbeiter in Bezug auf die Risiken. Das Risikobewusstsein kann dabei beispielsweise durch die Formulierung von risikopolitischen Grundsätzen gefördert werden. Die risikopolitischen Grundsätze sind ein Anstoß zur Etablierung eines Risikobewußtseins der Mitarbeiter und fördern die Risikokultur im Unternehmen. Dabei handelt es sich um dokumentierte Verhaltensregeln, welche die Mitarbeiter eines Unternehmens zu einem vernünftigen Umgang mit Risiken anleiten (vgl. http://www.kpmg.de/services/ business_services/pdf/IRM.pdf).

Das nötige Risikobewusstsein kann dabei nur in begrenztem Maß durch ausdrückliche Anweisungen, Kontrollmaßnahmen und Sanktionsmechanismen erreicht werden. „Risikobewußtsein ist vielmehr Ausdruck einer risikoorientierten Unternehmenskultur." (http://www.kpmg.de/services/ business_services/pdf/IRM.pdf) Die Risikokultur darf also nicht losgelöst von der Unternehmenskultur betrachtet werden. Sie ist vielmehr Teil der Unternehmenskultur[23]. Ihre Förderung liegt damit im Verantwortungsbereich der Unternehmensführung. Tatsächlich kann eine Risikokultur in einem Unternehmen nur dann etabliert und gefördert werden, wenn das Management dahinter steht. Oft müssen zu diesem Zweck erst verhaltensbedingte Barrieren überwunden werden. Dies kann z.B. durch ein Risikoberichtswesen als Transparenz schaffendes Instrument erreicht werden (vgl. Kirchner 2002, S. 19).

Auch aus diesem Grund ist die Risikokommunikation ein wichtiger Bestandteil einer Risikokultur. Gegenstand der Risikokommunikation ist die effiziente Nutzung von Risiko-Know-how und –Erfahrungen. Dabei sollte der Informationsaustausch ungehindert über Geschäfts- und geografische Grenzen sowie Hierarchiestufen stattfinden. Die Risikokommunikation sollte als offene Kommunikation verstanden werden und sowohl vertikal als auch horizontal ihre Anwendung finden. Dadurch ermöglicht eine wirkungsvolle Risikokommunikation eine zeitnahe Kommunikation von Sachverhalten, Risikotransparenz und die Förderung von schnellen Entscheidungen (vgl. Wallmüller 2004, S. 20).

Die Risikokultur eines Unternehmens wird besonders vom Managementstil und Umgang mit Risiken durch die Geschäftsleitung beeinflusst. Die Unternehmensleitung erfüllt also eine wichtige Vorbildfunktion.

---

[23] „Die Unternehmenskultur ist ein soziales Gebilde, das auf Werten und Erfahrungen basiert, das die Grundlage für die Interpretation der Wirklichkeit durch die Mitarbeiter ist und das zugleich ihre Interessen und ihr Handeln bestimmt." (Kirchner 2002, S. 19)

Risiken und Kontrollstrukturen müssen dabei ausgewogen bleiben. Übertriebene Kontrollen können langfristig genauso schädigend sein wie zu geringe Kontrollstrukturen (vgl. http://www.kpmg.de/services/ business_services/pdf/IRM.pdf).

Es lassen sich verschiedene Risiko-Management-Stile unterscheiden, aus denen sich verschiedene Risikokulturtypen ableiten lassen. Wie hoch Risiken in einer Organisation eingestuft werden, hängt mitunter auch vom Kulturtyp ab. Der Vorgang der Risikobewertung ist deshalb immer auch im Kontext der Risikokultur eines Unternehmens zu sehen (vgl. Junginger 1999, S. 18).

Die nachfolgende Abbildung gibt einen Überblick über mögliche Risiko-Management-Stile.

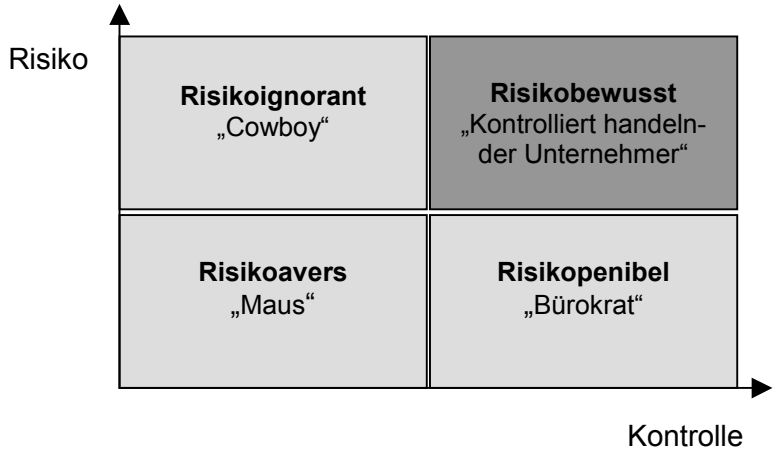


Abbildung 10: Risiko-Management-Stile (Quelle: http://www.kpmg.de/services/ business_services/pdf/IRM.pdf)

Für das Risiko-Management ist ein risikobewusster Management-Stil förderlich. Ist eine Unternehmensführung risikobewusst, sieht sie die Auseinandersetzung mit geschäftsbedingten Risiken als Notwendigkeit, um die erfolgreiche Umsetzung von Projekten zu fördern.

4.3 Prozess des Risiko-Managements

In den vorangegangenen Kapiteln wurde geklärt, was unter dem Begriff Risiko-Management zu verstehen ist und welche Rolle eine Risikokultur für das Risiko-Management spielt. Nun stellt sich die Frage nach der praktischen Vorgehensweise des Risiko-Managements.

Um auf dem aktuellen Stand der Risikobewältigung zu sein, muss sich das Risiko-Management immer wieder erneuern, damit auch neue bisher nicht definierte Risiken erkannt werden können. Deswegen muss das Risiko-Management in Form eines Regelkreislaufes stattfinden. Es ist keine einmalige Angelegenheit, sondern ein fortlaufender Prozess, der sich ständig wiederholt.

Dieser Regelkreislauf wird als Risiko-Management-Prozess bezeichnet. Er umfasst alle Aktivitäten zum systematischen Umgang mit Risiken.

Die wesentlichen Elemente des Risiko-Management-Prozesses sind die Identifikation, die Bewertung, die Steuerung und die Überwachung der Risiken. Der Risiko-Management-Prozess stellt den Mittelpunkt des Risiko-Managements dar (vgl. Kirchner 2002, S. 37).

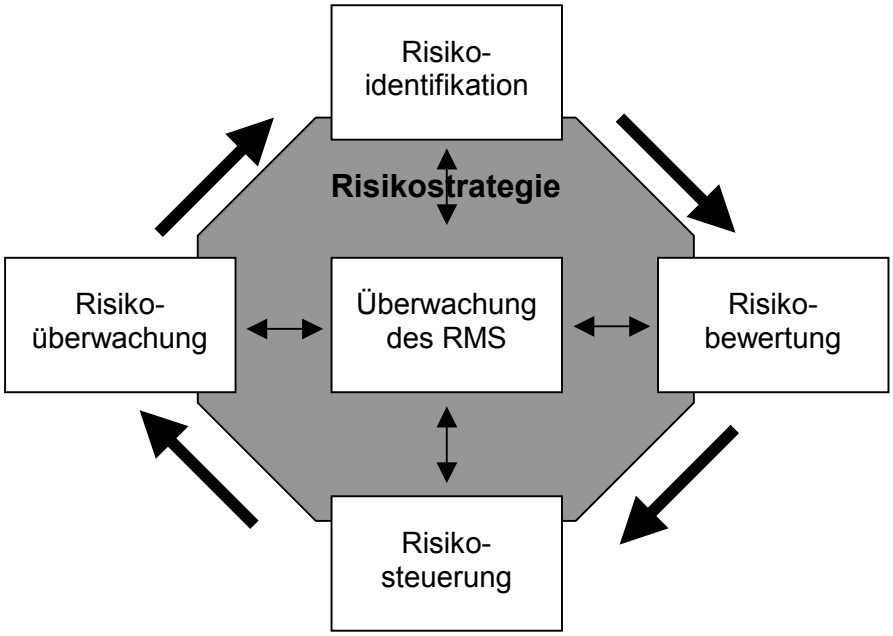


Abbildung 11: Prozess des Risiko-Managements (Quelle: In Anlehnung an http://www.kpmg.de/services/ business_services/pdf/IRM.pdf und Junginger (1999), S. 17)

4.3.1 Risikoidentifikation

Die Risikoidentifikation ist der erste wesentliche Schritt bei allen Risiko-Management-Prozessen. Sie ist dabei einer der schwierigsten Teile des Risiko-Management-Prozesses, da alle weiteren Maßnahmen auf ihr beruhen. Schließlich können nur die Risiken bewertet und gesteuert werden, die im Vorfeld erkannt wurden. „Es gilt die Regel, dass ein Risiko, das nicht im Vorfeld erkannt werden konnte, beim Eintreten auch nicht mit entsprechenden Maßnahmen in den Griff bekommen werden kann“ (Versteegen 2003, S. 67). Der Gesamterfolg des Risiko-Management-Prozesses wird also maßgeblich von der Qualität der Risikoidentifikation bestimmt. Als Mindestanforderungskriterien an die Phase der Risikoidentifikation können dementsprechend Vollständigkeit, Aktualität und Kontinuierlichkeit genannt werden (vgl. Kirchner 2002, S. 39). Vollständigkeit bedeutet dabei eine vollständige Erfassung von Risiken eines Projekts. Unter Aktualität wird eine zeitnahe Erfassung von Risiken verstanden. Da sich Risiken durch z.B. veränderte Rahmenbedingungen auch ändern können, muss, um die Kriterien der Vollständigkeit und Aktualität erfüllen zu können, das Kriterium der Kontinuierlichkeit herangezogen werden. Darunter ist zu verstehen, dass eine Risikoidentifikation in kontinuierlichen Abständen wiederholt werden muss.

Die Risikoidentifikation kann in Form einer Risikoinventur[24] stattfinden (vgl. Kirchner 2002, S. 39). Alle Risiken, die ein Projekt betreffen, können in der Risikoinventur gesammelt werden. Die gesammelten Risiken können dann beispielsweise in einer Risikoliste festgehalten werden.

Zur Erkennung der Risiken können verschiedene Hilfsmittel verwendet werden. Dazu gehören Checklisten, Interviews mit Fragebogen, Meetings und moderierte Workshops (vgl. Wallmüller 2004, S. 134). Checklisten sind ein leicht zu benutzender systematischer Weg zur Erkennung von Risiken. Ein Nachteil dabei ist, dass oft standardisierte Checklisten genutzt werden, die nicht für jeden Projekttyp und jede Projektsituation passend sind (vgl. Wallmüller 2004, S. 134). Um diesem Nachteil zu entgehen, können Checklisten speziell entwickelt werden. Diese Aufgabe könnte z.B. ein Risikobeauftragter übernehmen.

Bei Interviews befragt ein Interviewer eine Gruppe von Personen zu Risiken. Dies können z.B. Projektmitarbeiter sein. Der Interviewer ist dabei eine unabhängige Person, die vorher festgelegte Fragen stellt. Ein Vorteil dieser Methode ist, dass sich durch die Diskussion der Fragen, Synergien einstellen können (vgl. Wallmüller 2004, S. 134).

Zur Risikoerkennung sind weiter auch Meetings, wie z.B. Statusmeetings und Projekt-Reviewsitzungen, geeignet. Für die Meetings sollte zu diesem Zweck ausreichend Zeit zur Diskussion von Risiken eingeräumt werden.

Moderierte Workshops sind schließlich eine weitere Möglichkeit zur Risikoerkennung. Sie haben den Vorteil, dass Risiken situationsgerecht und umfassend gefunden werden können. Zur Erkennung von Risiken werden Brainstormings, Nachdenken oder Modellierung bzw. Simulation verwendet (vgl. Wallmüller 2004, S. 136).

Die genannten Hilfsmittel können auch kombiniert werden. So kann die Kombination aus moderierten Workshops und dem Einsatz von Checklisten ein wirksames Vorgehen sein (vgl. Wallmüller 2004, S. 136).

Durch diese Hilfsmittel können zahlreiche Risiken identifiziert werden. Die Einteilung der Risiken in Risikokategorien ist ein Weg, Übersicht über die entdeckten Risiken zu bekommen. Eine saubere Abgrenzung der relevanten Risikokategorien muss für eine Bewertung der Risiken durchgeführt werden.

Im Falle eines unternehmensweiten Risiko-Managements lassen sich die Risiken grundsätzlich in drei Hauptkategorien unterteilen: in Risiken des leistungswirtschaftlichen Bereichs, des finanzwirtschaftlichen Bereichs und solche aus dem Corporate Governance und des Managements (vgl. Romeike/Finke 2003, S. 168). Des weiteren können auch aus internen und externen Ereignissen und Störungen Risiken entstehen. Aufgrund der Vielschichtigkeit und Komplexität ist die Abgrenzung zwischen den Risikokategorien oft sehr schwierig (vgl. Romeike/Finke 2003, S. 168).

[24] Die Risikoinventur wird auch als Risikobestandsaufnahme bezeichnet.

Im Falle eines Risiko-Managements bei Projekten können diese Risikokategorien herangezogen werden. Wegen der Komplexität, die Projekte annehmen können, werden aber häufig eigene projektspezifische Risikokategorien entwickelt.

4.3.2 Risikobewertung

Hat man die Risiken mit Hilfe der Risikoidentifikation erkannt, müssen sie in einem nächsten Schritt analysiert und bewertet werden. Die Aufgaben der Risikobewertung sind die Feststellung der Eintrittswahrscheinlichkeit der Risiken und die Ermittlung möglicher Auswirkungen, falls ein Risiko eintreten sollte (vgl. Versteegen 2003, S. 101).

Eine Abhängigkeit zwischen Risiken ist möglich. Ein Risiko tritt in so einem Fall erst dann ein, wenn zuvor ein anderes eingetreten ist. Dieser Sachverhalt ist in der Risikobewertung ebenfalls von Bedeutung. So kann es von Vorteil sein bestimmte Risiken unabhängig von Eintrittswahrscheinlichkeit und Auswirkungen zusätzlich als bedeutendes Risiko einzustufen. Der Grund dafür liegt in der Wirkung, die einzelne Risiken auf andere haben können. Diese Wechselbeziehungen sollten bei der Bewertung auch berücksichtigt werden (vgl. Kirchner 2002, S. 41).

Die Motivation einer Risikobewertung liegt dabei in der Fülle an potenziellen Risiken. Da nicht für jedes einzelne Risiko[25] sämtliche Planungsmaßnahmen, wie Verhinderung, Verringerung, Schadensbegrenzung und Notfallplanung durchgeführt werden können ist eine Differenzierung zwischen Primär- und Sekundärrisiken sinnvoll (vgl. Kirchner 2002, S. 41). Risiken mit hohem Schadenspotenzial können dadurch hervorgehoben werden. Zu diesem Zweck ist eine qualitative Beurteilung bzw. quantitative Messung der Risiken notwendig. Dadurch kann auch ein Risikoportfolio für Unternehmensrisiken aber auch für Risiken von komplexen Projekten erstellt werden. Zur Bewertung der Risiken können Werte für die Risikoattribute Wahrscheinlichkeit (z.B. finanzieller Verlust) und Auswirkungen des Eintretens definiert werden. Die Beurteilung der Eintrittswahrscheinlichkeit ist subjektiv. Es ist deshalb sinnvoll, dass die Durchführung der Risikobewertung von einem Team durchgeführt wird. Mehrere Personen können so ihre (subjektive) Meinung der Eintrittswahrscheinlichkeit eines konkreten Risikos abgeben (vgl. Versteegen 2003, S. 102).

Ebenso, wie die Eintrittswahrscheinlichkeit, sollten auch die Auswirkungen quantifiziert werden. Unter Auswirkungen sind dabei im Falle eines Projektes alle negativen Einwirkungen auf das Vorhaben zu verstehen. Diese können sich beispielsweise auf die Kosten / Finanzen, den Zeitplan oder die technische Leistungsfähigkeit beziehen. So können zusätzliche Kosten entstehen, die sich aus Terminverzögerungen oder nicht erreichter Zielvereinbarungen ergeben.

---

[25] Das gilt sowohl für allgemeine Unternehmensrisiken als auch für spezielle Projekte, wie dem IT-Outsourcing.

Hilfsmittel für die Risikobewertung sind z.B. das Risikoerfassungsformular und die Risikomatrix. Ein Risikoerfassungsformular dient zur Erfassung und Bewertung von Risiken. Es kann beispielsweise folgendermaßen gestaltet sein.

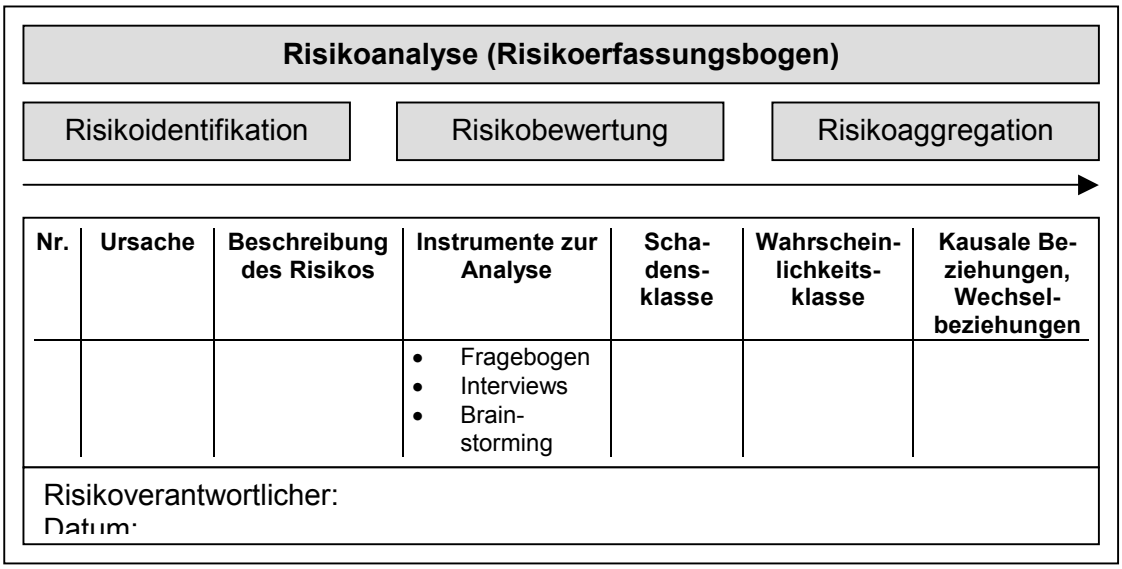


Abbildung 12: Beispiel für ein Risikoerfassungsformular (Quelle: Kirchner 2002, S. 40)

Mit Hilfe des Risikoerfassungsformulars können Risiken gesammelt und bewertet werden. Die Sammlung von Risikodaten durch Risikoerfassungsformulare kann dabei durch einfache Datenbanken realisiert werden.

Ein weiteres Hilfsmittel, dass angewendet werden kann, ist die Risikomatrix. Basis für die Risikomatrix sind die Risikoliste der Risikoidentifikation und allgemein die Risikoanalyse (vgl. Versteegen 2004, S. 131). Alle identifizierten Risiken werden in die Risikomatrix eingegliedert und anschließend bewertet und gegenübergestellt. Ziel der Risikomatrix ist die Übersicht über die identifizierten Risiken und deren Bewertung. Beim Projekt-Management dient sie dabei in erster Linie dazu, einen aktuellen Überblick zu geben, wie sich die Risikosituation in einem Projekt gestaltet. Aus diesem Grund sollte sie bei einem Einsatz ständig gepflegt und aktuell gehalten werden. Eine Risikomatrix setzt sich aus den zwei Elementen Risikoklassen und Risikowahrscheinlichkeitsklassen zusammen (vgl. Versteegen 2004, S. 131).

Durch die Risikoklassen erfolgt eine Einordnung der Risiken im Hinblick auf die Schwere eines Risikos, also der Auswirkungen, die durch das Eintreten entstehen. Die Risikowahrscheinlichkeitsklassen wiederum beschreiben die Wahrscheinlichkeit hinsichtlich des Eintretens von Risiken.

In der Praxis haben sich folgende Risikowahrscheinlichkeitsklassen als anwendbar herausgebildet (vgl. Versteegen 2004, S. 136):

- RWK 1: Das Eintreten des Risikos ist durchaus wahrscheinlich.
- RWK 2: Das Eintreten des Risikos ist möglich.
- RWK 3: Das Eintreten des Risikos ist nur unter bestimmten Bedingungen möglich.
- RWK 4: Das Eintreten des Risikos ist eher unwahrscheinlich.
- RWK 5: Das Eintreten des Risikos ist nahezu ausgeschlossen.

Auch die Abhängigkeiten von Risiken lassen sich durch die Risikomatrix darstellen.

Eine Risikomatrix kann beispielsweise folgendermaßen aussehen:

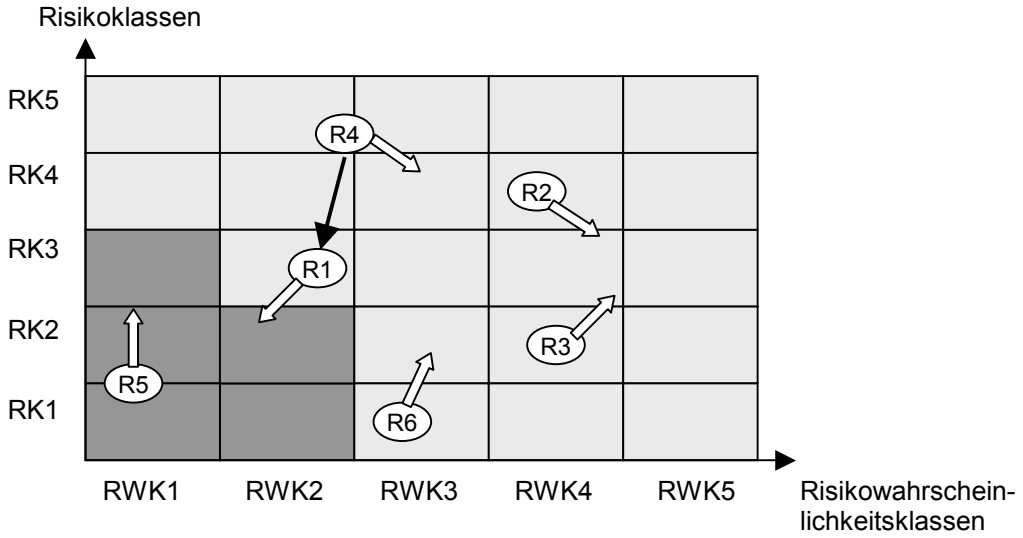


Abbildung 13: Beispiel für eine Risikomatrix (Quelle: In Anlehnung an Versteegen 2003, S. 146 und S. 149)

Die Risikoidentifikation und die Risikobewertung werden oft zusammen als Risikoanalyse bezeichnet. Inhalt der Risikoanalyse ist dabei die qualitative Bewertung und quantitative Messung von Risiken einschließlich ihrer Zusammenhänge. Die Risikoanalyse liefert damit die Informationsbasis für die weiteren Prozessschritte des Risikomanagements und insbesondere der Risikosteuerung.

4.3.3 Risikosteuerung

Unter Risikosteuerung versteht man die aktive Beeinflussung, der im Rahmen der Risikoidentifikation und Risikobewertung ermittelten Risiken entsprechend ihrer Risikoposition. Voraussetzung für eine effektive Risikosteuerung ist eine regelmäßige Erfassung der Analyseergebnisse und eine sachgerechte Informierung der Entscheidungsträger (vgl. http://www.kpmg.de/services/ business_services/pdf/IRM.pdf). Die Maßnahmen, die für die Steuerung getroffen werden, haben dabei eine Verringerung der Eintrittswahrscheinlichkeit und/oder eine Begrenzung der Auswirkungen zum Ziel.

Die ergriffenen Steuerungsmaßnahmen sollen dazu beitragen nicht akzeptable Risiken zu vermeiden und Risiken, die sich nicht vermeiden lassen auf ein Maß zu reduzieren, dass akzeptabel ist. Im Rahmen der Risikosteuerung wird für jedes Einzelrisiko, das in der Risikoidentifikation ermittelt wurde, eine Risikostrategie festgelegt. Jedes Risiko wird dabei mit nur einer Strategie bearbeitet. Eine Strategie kann jedoch für mehrere Einzelrisiken angewendet werden (vgl. Versteegen 2003, S. 167f).

Grundsätzlich stehen zur Steuerung von Risiken vier Strategiealternativen zur Verfügung, die an dieser Stelle näher beschrieben werden sollen.

Die Risikostrategien, die zur Verfügung stehen sind

- die Risikovermeidung,
- die Risikoakzeptierung,
- die Risikominimierung und
- die Risikoübertragung.

Gegenstand der Risikovermeidung ist die Vermeidung des Eintretens von Risiken. Für diese Strategie kommen allerdings nur diejenigen Risiken in Betracht, deren Auswirkungen beim Eintreten gravierend wären. Hauptgrund dafür ist die Kostenintensivität zur Vermeidung solcher Risiken (vgl. Versteegen 2003, S.174)

Hat man ein Risiko entdeckt, das vermieden werden sollte, ist ein Maßnahmenkatalog zur Vermeidung des Risikos zu erstellen. Die Kosten[26], die dabei für jede Maßnahme entstehen, sollten in den Katalog miteinbezogen werden.

Ergänzend zur Risikostrategie der Vermeidung kann der Risikoschutz als zusätzliche Kategorie genannt werden (vgl. Versteegen 2003, S.171). Typische Beispiele sind vor allem im technologischen Bereich zu finden. Dazu zählen die Einrichtung von Firewalls, die Integration eines verstärkten Qualitätsmanagements, die Beschaffung spezieller Software usw.. Um herauszufinden, ob solche Investitionen im Einzelfall gerechtfertigt sind, ist die Einbeziehung der Auswirkungen der Risiken notwendig. Sind die Auswirkungen weniger gravierend, kann auf andere Risikostrategien ausgewichen werden. Typische Einsatzfelder der Strategie der Risikovermeidung[27] sind Technologierisiken, Sicherheitsrisiken und Vertragsrisiken (Versteegen 2003, S.173).

Zu den defensivsten Strategien innerhalb des Risikomanagements gehört die Strategie der Risikoakzeptierung. Risikoakzeptierung bedeutet letztendlich die Akzeptanz des Eintretens eines Risikos.

---

[26] In vielen Fällen bilden die Kosten die Entscheidungsgrundlage für die Wahl der Risikostrategie. Oft wird dabei den kostengünstigeren Lösungen, wie die Riskoakzeptierung der Vortritt gegeben.

[27] Ein interessanter Aspekt bei der Risikovermeidung ist, dass diese Strategie bei der Anwendung selbst eine Reihe von Problemen und Risiken birgt. Ein Beispiel dafür ist, dass sich Risiken wie „Rückgang der Motivation der Projektmitarbeiter“ schwer einschätzen lassen. (vgl. Versteegen 2003, S. 172) Für weitere Beispiel diesbezüglich soll an Versteegen (2003) verwiesen werden.

Diese Strategie wird angewendet, wenn Risiken aufgrund ihres Schadensausmaßes und ihrer Eintrittswahrscheinlichkeit als gering eingestuft sind (vgl. http://www.kpmg.de/services/ business_services/pdf/IRM.pdf).

Deswegen werden nur bedingt vorbeugende Maßnahmen getroffen z.B. durch die Erstellung eines groben Maßnahmenkatalogs. Im Rahmen der Risikoakzeptierung sind zwei Ansätze zu unterscheiden (vgl. Versteegen 2003, S. 175):

- Risikoakzeptierung mit Notfallplanung
- Risikoakzeptierung ohne Notfallplanung

Unter Notfallplanung ist dabei ein Maßnahmenkatalog zu verstehen, der die Aktivitäten beinhaltet, die beim Eintreten eines Risikos eingeleitet werden sollten.

Die Strategie der Risikoakzeptierung ist nur für erfahrene Risikomanager oder Projektleiter geeignet. Eine falsche Einschätzung der Risikoposition kann nämlich u. U. zu einer Krise oder direkt zu einem Problemfall führen. Vorteil dieser Strategie hingegen ist die Ersparnis von Zeit und Kosten.

Als Mittelweg zwischen Risikovermeidung und Risikoakzeptierung ist die Risikominimierung zu verstehen. Zum einen ist sie nicht so kostspielig, wie die Risikovermeidung und zum anderen nicht so riskant, wie die Risikoakzeptierung. In der Literatur werden oft zwei Ansätze der Risikominimierung unterschieden. Der erste Ansatz verfolgt die Möglichkeiten zur Verringerung der Eintrittswahrscheinlichkeit, während sich der zweite der Minimierung der Auswirkungen eines eingetretenen Risikos widmet. Eine der wesentlichsten Möglichkeiten zur Risikominimierung ist die Integration von Vertragsklauseln[28] (vgl. Versteegen 2003, S.177).

Eine weitere mögliche Risikostrategie ist die Risikoübertragung. Grundlage dieser Strategie ist die Übertragung von einer Vielzahl von Risiken an eine dritte Partei (vgl. Romeike/Finke 2003, S. 237). Diese kann z.B. ein externes Unternehmen sein. Dabei ist Ziel dieser Strategie nicht nur Risiken zu vermeiden, sondern auch die Auswirkungen beim Eintreten eines Risikos auf eine dritte Partei zu verlagern. Eine einfache aber kostspielige Möglichkeit zur Risikoübertragung ist der Transfer von Risiken auf ein Versicherungsunternehmen (vgl. Versteegen 2003, S.182)). Die meisten Versicherungen konzentrieren sich dabei auf die Produkthaftung. Die Strategie der Risikoübertragung ist in der Regel sehr aufwendig, kann aber zusätzliche Sicherheit und Kostenersparnisse bringen, da die Kosten zur Steuerung der übertragenen Risiken von der dritten Partei getragen werden müssen. Bei der Risikoübertragung gilt generell, dass ein Risiko zwar übertragen werden kann, damit jedoch nicht vermieden wurde.

Zusammenfassend lässt sich sagen, dass spätestens bei der Risikosteuerung deutlich wird, dass nur diejenigen Risiken gesteuert werden, die im Rahmen der Risikoidentifikation erkannt wurden. Eine kontinuierliche Risikoerkennung ist deshalb nötig.

28 Beim IT-Outsourcing sind die SLAs ein Beispiel dafür. Vgl. dazu Kapitel 2.5.3

Auch kann aus einer falschen Bewertung eines Risikos die Wahl einer falschen Risikostrategie resultieren. Je nach den daraus entstehenden Konsequenzen kann das verheerende Auswirkungen haben.

Für Projekte gilt der Grundsatz, dass mehrere Strategien zum Einsatz kommen sollten. Die Strategien finden ihre Anwendung dabei nicht projektbezogen, sondern für jedes erkannte Risiko.

4.3.4 Risikoüberwachung

Auch durch die Anwendung von Maßnahmen zum Umgang mit Risiken bleibt dennoch ein Restrisiko zu tragen.

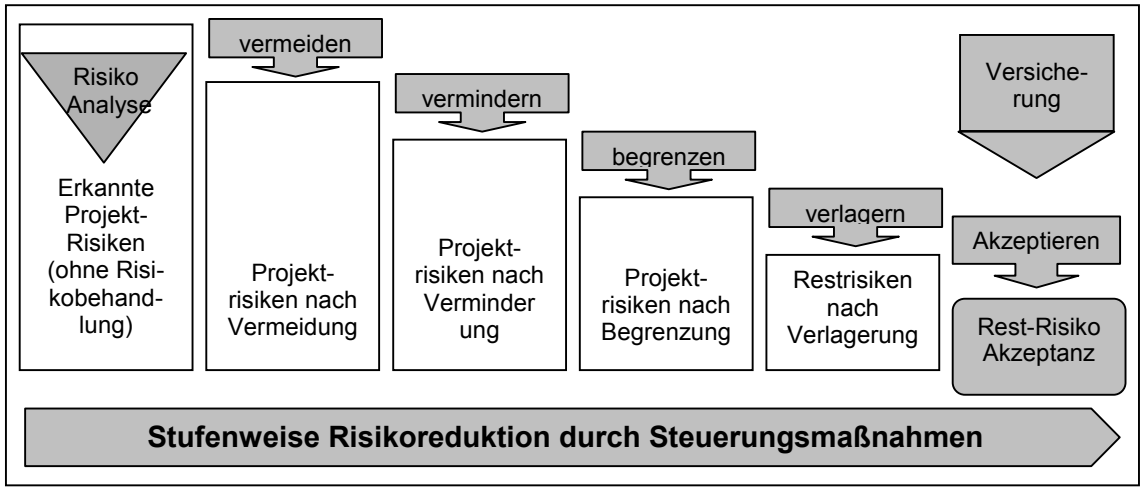


Abbildung 14: Risikomaßnahmen (Quelle: Hodel/Berger/Risi 2004, S.152)

Die letzte Stufe des Risikomanagement-Prozesses - sofern bei einem Kreislauf von einer letzten Stufe gesprochen werden kann – bildet die Risikoüberwachung. Zentrum der Risikoüberwachung ist dabei die „kontinuierliche operative Kontrolle der Wirksamkeit der Risikosteuerungsmaßnahmen“ (http://www.kpmg.de/services/ business_services/pdf/IRM.pdf). Instrumentell wird diese Aufgabe durch Abweichungsanalysen bzw. Soll-Ist-Analysen unterstützt. Die Definition von Kennzahlen und Indikatoren ist zu diesem Zweck sinnvoll. Dabei können Schwellen- bzw. Toleranzwerte festgesetzt werden. Bei Überschreitung dieser kann eine Meldung z.B. an einen Risikobeauftragten veranlasst werden. Dieser kann in einem nächsten Schritt die Informationen bündeln und an die Geschäftsleitung weitergeben. Eine besondere Bedeutung kommt dabei der zeitnahen Weitergabe der Risikoinformationen zu (vgl. Kirchner 2002, S. 51).

Bei einem Risikomanagement bei Projekten sollte auch eine Weitergabe an das unternehmensweite Risikomanagement stattfinden. Dort können die Risikoinformationen gesammelt, aggregiert und für eine unternehmensweite Auswertung zur Verfügung gestellt werden.

4.3.5 Regelkreislauf und Dokumentation

Durch die einmalige Identifikation von Risiken ist lediglich der Beginn des Risiko-Management-Prozesses eingeläutet. Für eine aktuelle und permanente Überprüfung der Risiken muss die Risikoidentifikation und damit der gesamte Risiko-Management-Prozess regelmäßig wiederholt werden. Um Transparenz über diesen Prozess zu gewährleisten, dient die Dokumentation. Mit ihrer Hilfe kann sich der Aufbau und der Inhalt des Risiko-Management-Prozesses verdeutlichen lassen (vgl. Kirchner 2002, S. 71) Die beteiligten Mitarbeiter können den Regelkreislauf so besser nachvollziehen.

Ziel der Risikodokumentation ist also die Transparenz und Nachvollziehbarkeit von Ergebnissen und Maßnahmen. Aus diesem Grund sollten alle Phasen des Risiko-Management-Prozesses dokumentiert werden. Als Anforderungskriterien lassen sich dabei die Vollständigkeit, die Aktualität und die Verfügbarkeit nennen (vgl. Junginger 1999, S. 98). Bezieht man diese Anforderungskriterien der Dokumentation auf ein Risiko-Management bei Projekten, dann erfordert die Erfüllung des Kriteriums Vollständigkeit, eine vollständige Erfassung aller potentiellen Risiken eines Projektes. Die Aktualität ist dem Kriterium der Vollständigkeit übergeordnet. Einmal identifizierte, analysierte und gesteuerte Risiken sollten nicht als statisches Ergebnis aufgefasst werden, sondern verlangen eine kontinuierliche Wiederholung. Unter Verfügbarkeit ist wiederum gemeint, dass die Dokumentation unabhängig von Hierarchie, Ort und Zeit zur Verfügung gestellt wird. Dadurch werden auch die Kriterien der Vollständigkeit und Aktualität unterstützt.

Eng verknüpft mit der Dokumentation ist das Berichtswesen. Dabei ist vor allem an das Berichtswesen im Hinblick auf z.B. den Aufsichtsrat oder die Jahresabschlussprüfung zu denken. So kann ein Risikoberichtswesen als Basis für eine ausreichende Selbstinformation des Managements genutzt werden (vgl. Kirchner 2002, S. 71). Ein Projekt kann so seiner Nachweispflicht gegenüber der Geschäftsleitung nachkommen.

Für eine effektive Dokumentation und Berichterstattung ist es sinnvoll IV-Systeme heranzuziehen. Standardtools, wie beispielsweise MS Excel, MS Word und MS Access[29], können dazu herangezogen werden (vgl. Versteegen 2003, S. 91). Das Angebot an speziellen Software-Tools hat sich im Laufe der Jahre zwar verbessert, ist heutzutage dennoch gering[30].

4.4 IT-Risiko-Management

Nachdem nun Grundlagen des Risiko-Managements erläutert wurden, soll an dieser Stelle auch auf das IT-Risiko-Management eingegangen werden. Hauptgegenstand des IT-Outsourcing ist letztendlich die Informationstechnologie, wodurch das IT-Risiko-Management unmittelbar betroffen ist.

---

[29] MS Word, MS Excel und MS Access sind eingetragene Warenzeichen der Microsoft Coorperation.

Zu erwähnen ist dabei, dass ebenso wie das Risiko-Management bei Projekten auch das IT-RM[31] nicht losgelöst vom allgemeinen Kontext des Risiko-Managements gesehen werden darf. Es dient lediglich der Reduktion von Komplexität im Rahmen dieser Arbeit, nur auf die relevanten Bereiche im Hinblick auf die IT-Outsourcing-Thematik einzugehen.

4.4.1 Datenschutz und Datensicherheit

Zu den klassischen Schwerpunkten im Umgang mit Risiken gehören der Datenschutz und die Datensicherheit. Aus diesem Grund soll an dieser Stelle auf diese Punkte eingegangen werden.

Unter dem Begriff Datenschutz ist zunächst der Schutz von personenbezogenen Daten vor unbefugtem Zugriff oder missbräuchliche Verwendung zu verstehen. Datenschutz ist dabei eine gesetzlich reglementierte Vorgehensweise bzw. Vorgabe, die dann zum Einsatz kommt, wenn durch ein Unternehmen, eine Institution oder eine Person Daten von Dritten gesammelt, aufgezeichnet und/oder verarbeitet werden (vgl. Edelbacher/Reither/Preining 2000, S. 258).

§1, Abs. 1 des BDSG lautet deshalb:

„Aufgabe des Datenschutzes ist es, durch den Schutz personenbezogener Daten vor Missbrauch bei der Speicherung, Übermittlung, Veränderung und Löschung (Datenverarbeitung) der Beeinträchtigung schutzwürdiger Belange der Betroffenen mitzuwirken."

Vor dem Hintergrund der wachsenden Erfassung von persönlichen Daten in Rechnersystemen, der Massendatenverarbeitung und der steigenden Verfügbarkeit in elektronischen Datenbanken gewinnt der Datenschutz dabei an Bedeutung. Konzeptbedingt wird mit der Bereitstellung von Informationen in elektronischer Form auch der unberechtigte Zugang zu diesen Informationen ermöglicht. Der Datenschutz ist heutzutage deshalb vor allem auch mit Forderungen an die Informationsverarbeitung verbunden (vgl. Junginger 1999, S. 21).

Die Datensicherung beschäftigt sich im Gegensatz zum Datenschutz mit allen „organisatorischen und technischen Maßnahmen, die bei der Speicherung, Verarbeitung und Weitergabe von Informationen diese vor Verlust, Zerstörung oder Missbrauch bewahren. Als Datensicherheit bezeichnet man den Zustand, der durch Maßnahmen der Datensicherung erreicht wird" (Krallmann 1989, S. 15).

---

[30] Im Anhang ist ein Überblick über Standardtools zu finden.

[31] Die Instrumente und Methoden die im Rahmen des Risiko-Managements für Projekte erläutert wurden, gelten auch für das IT-Risiko-Management. Lediglich der Blickwinkel ist anders und liegt nicht beim Projekt, sondern bei der IT.

Das Thema Datensicherheit wird um so bedeutender, je mehr sich Unternehmen nach außen hin öffnen. Dies kann durch das Internet[32] stattfinden, aber auch durch ein Outsourcing der IT. Die Sicherheit der IT wird dann zum zentralen Thema. Heutzutage gibt es für viele Gefahren spezielle technische Lösungen, die das Risiko einer unlauteren Verwendung verringern. Die nachfolgende Tabelle gibt einen Überblick über die möglichen Gefahren, die technischen Maßnahmen und deren Kosten-Nutzen-Verhältnis.

Gefahr	Maßnahme	Kosten	Nutzen
Datenverlust, Downtime	Archivierung Datensicherung Replikation Load Balancing	Niedrig Niedrig Mittel Mittel	Hoch Hoch Hoch Hoch
Unberechtigter Zugang	Zutrittsschutz Berechtigungswesen Single-Sign-On Digitale Identitäten Firewall	Hoch Hoch Niedrig Mittel Hoch	Mittel Hoch Hoch Sehr hoch Hoch
Elektronischer Betrug	Elektronische Unterschrift	mittel	Hoch
Zugriff auf Kommunikationsdaten	VPN SSL E-Mail-Verschlüsselung Verschlüsselung der Applikationskommunikation	**Hoch** **Niedrig** **Mittel** **mittel**	Niedrig Hoch Hoch Hoch

Tabelle 2: Gefahren, technische Maßnahmen und deren Kosten-Nutzen-Verhältnis (Quelle: Dörner/Horváth/Henning 2000, S. 409)

Zu erwähnen ist, dass auch bei technischen Maßnahmen Restrisiken bleiben. Dazu gehört der Risikofaktor Mensch. Technische Maßnahmen helfen nur bedingt gegen unlautere Mitarbeiter. Eine weitere Zielsetzung im Hinblick auf Datensicherheit muss deshalb die Motivation zur Verantwortung und zur Beachtung der Sicherheitsrichtlinien sein.

4.4.2 Ganzheitliche Sicht auf das IT-Risiko-Managements

In der Praxis beschränkt sich die Betrachtung der IT-Risiken meistens auf die klassischen Schwerpunkte der Sicherheit und der rechtlich verbindlichen Regelungen. Nur selten wird das IT-RM als Bestandteil einer integrativen Unternehmensstrategie gesehen. Für eine wirksame Analyse und Kontrolle der IT-Risiken ist eine ganzheitliche Sicht allerdings sinnvoll (vgl. Junginger 1999, S. 20).

Um eine ganzheitliche Sicht auf die relevanten Risiken auf dem Gebiet der IT zu bekommen, kann das Ebenenmodell des Informationsmanagements nach Krcmar herangezogen werden. Junginger hat diesen Sachverhalt aufgegriffen und durch die nachfolgende Abbildung dargestellt.

[32] Ein Beispiel dafür ist, wenn Unternehmen eine direkte Integration ihrer Systeme in das Internet anstreben. Dabei kann es Ziel sein, die Vorteile des E-Business zu nutzen.

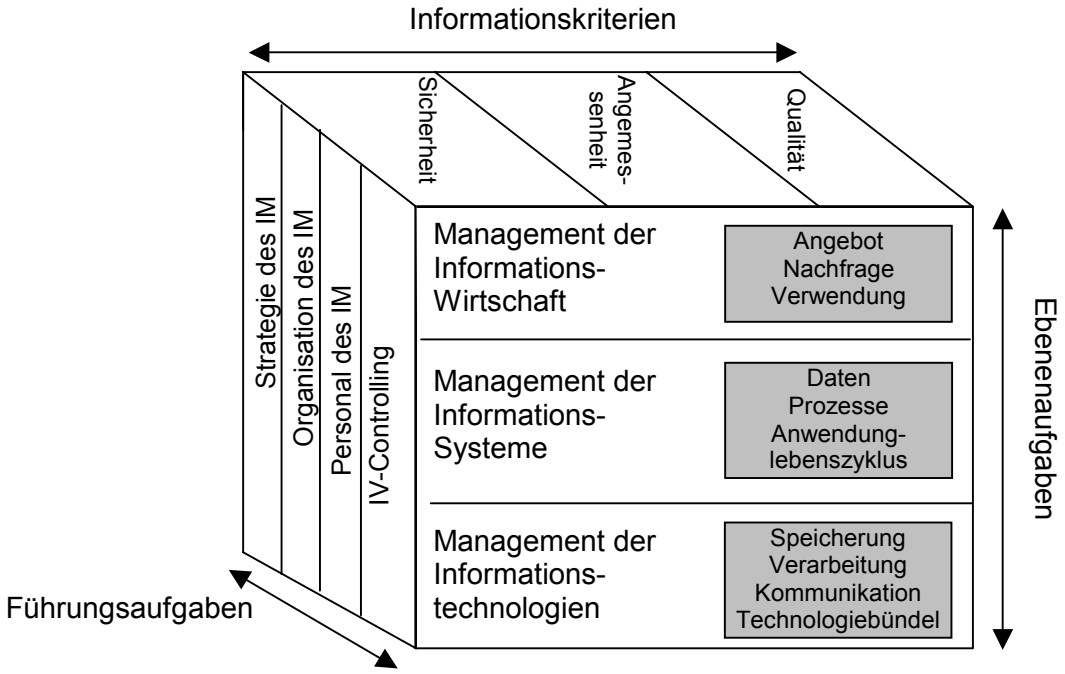


Abbildung 15: Erweitertes Modell des IM: Der Informationsmanagement-Würfel (Quelle: Junginger 1999, S. 48)

In dieser Abbildung sind die Aufgaben des IM in drei Dimensionen eingeteilt. In der ersten Dimension ist das IM eine auf drei Ebenen verteilte Managementaufgabe. Dabei handelt es sich um die Ebenen des Managements der Informationswirtschaft, der Informationssysteme und der Informationstechnologien. Die zweite Dimension beschreibt die Führungsaufgaben des IM und lässt sich nicht auf eine Ebene beschränken, sondern hat einen generellen Charakter (vgl. Junginger 1999, S. 48). Ergänzend kommt bei Junginger noch eine dritte Dimension dazu, welche ebenso wie die Führungsaufgaben einen Querschnittscharakter haben. Es handelt sich dabei um die Informationskriterien. Von jeder Ebene des Informationsmanagements gehen dabei spezifische Risiken aus. Dementsprechend lassen sich folgende Risikokategorien für den Bereich der IT ableiten (Junginger 1999, S. 2):

- „Risiken der Informationswirtschaft
- Risiken der Informationssysteme
- Risiken der Informationstechnologie
- Risiken der Führungsaufgaben“

Die Auswirkungen dieser Risiken zeigen sich z.B. in Informationspathologien, Prozessdiskfunktionalitäten und einer unzureichenden Verfügbarkeit der Informations- und Kommunikationstechnologien. (vgl. Krcmar 2003, S. 359)

Die einzelnen Risiken der Ebenen des Informationsmanagements können dabei nicht isoliert betrachtet werden, sondern haben einen interdependenten Charakter. Krcmar hat diesen Zusammenhang zwischen Aufgaben des IM und deren Interdependenzen durch nachfolgende Abbildung dargestellt.

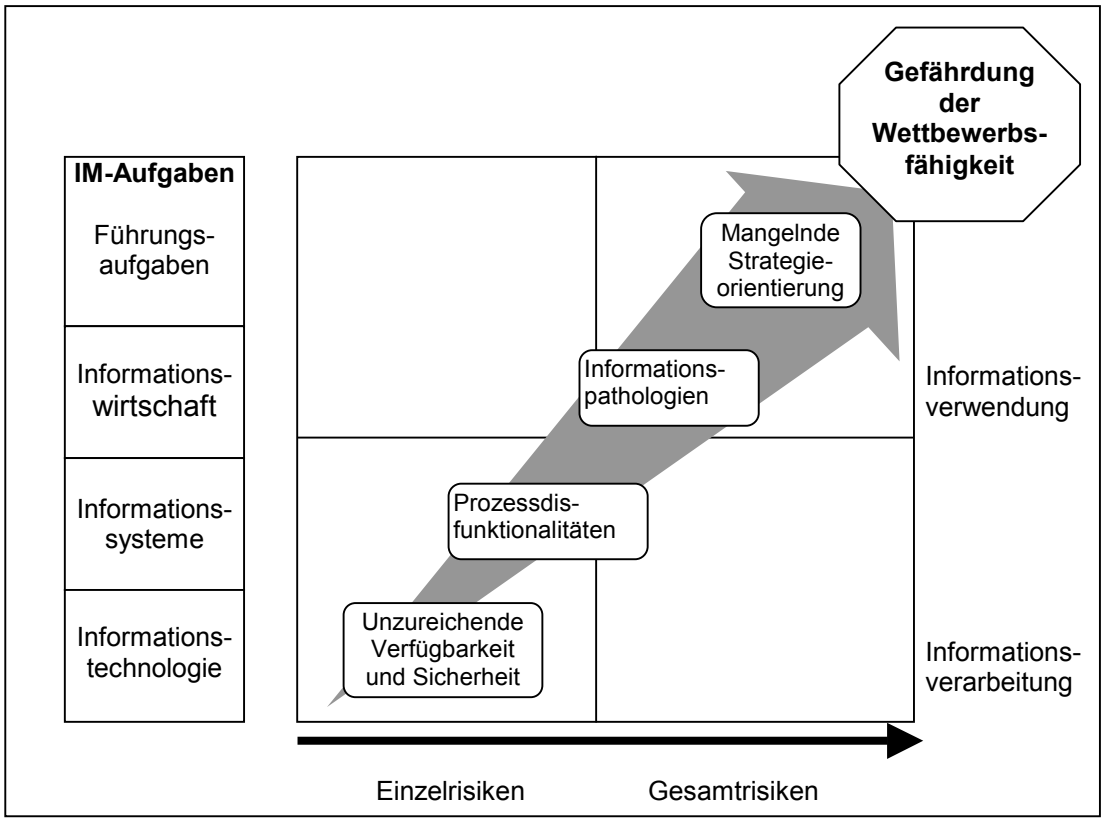


Abbildung 16: IT-Risiken und ihre Wirkungen (Quelle: Krcmar 2003, S. 360)

4.4.3 IT-Risiko-Management und IT-Outsourcing

Nun stellt sich an dieser Stelle die Frage, welche Bedeutung das IT-Risiko-Management für das IT-Outsourcing hat. Zweifellos geht aus der Abbildung 16 hervor, dass ein Eintreten von Risikopotentialen im Bereich der Informationstechnologie weitreichende Folgen für alle Ebenen des Informationsmanagements hat. Die Informationstechnologie als unterste Ebene bildet ein Fundament, auf dem die weiteren Ebenen aufbauen. Entsteht also eine negative Situation auf der Ebene der Informationstechnologie werden durch den interdependenten Charakter der Risiken alle weiteren Ebenen des Informationsmanagements ebenfalls betroffen (vgl. Krcmar 2003, S. 359). Die Folgen, die dadurch für ein Unternehmen entstehen, sind dabei abhängig von der Schwere eines aufgetretenen Risikos, können aber bis zur Gefährdung der Wettbewerbsfähigkeit reichen.

Möchte man die IT eines Unternehmens auslagern, muss diese Abhängigkeit bekannt und berücksichtigt werden und in das Risiko-Management des IT-Outsourcing-Projekts miteinbezogen werden. Auch wird die Verantwortung ersichtlich, die auf den Outsourcingnehmer übertragen wird. Es ist deshalb sinnvoll das IT-Risiko-Management bei der Realisierung eines solchen Vorhabens heranzuziehen, da der IT-Betrieb während des Outsourcing-Prozesses aber auch in der Betriebsphase gewährleistet sein sollte. Das IT-RM kann dazu beitragen die IT-Risiken zu minimieren.

4.5 Weitere dem Risiko-Management angelehnte Techniken

Wie in den vorangegangenen Kapiteln erläutert wurde, ist das Ziel des Risiko-Managements eine erfolgreiche Risikobewältigung. Einfach ausgedrückt, bedeutet dies, dass es stattfindet, bevor das passiert, was passieren könnte. Es ist also proaktiv und dient dazu, die Entscheidung zu ermöglichen, ob und wie mit Risiken umgegangen wird, ob sie vermieden werden oder ob sie bewusst eingegangen werden sollen. Ein kontrollierter Umgang mit Risiken soll dadurch gewährleistet werden. Aber auch bei funktionierenden Risiko-Management-Systemen können unerwünschte Risiken auftreten. Ist ein Risiko mit gravierenden Auswirkungen tatsächlich aufgetreten, kommen deshalb weitere Managementtechniken zum Einsatz. Zu nennen sind dabei das Krisen-Management und das Notfall-Management. Diese Managementtechniken resultieren aus dem Risiko-Management und werden aus diesem Grund oft im Zusammenhang gesehen.

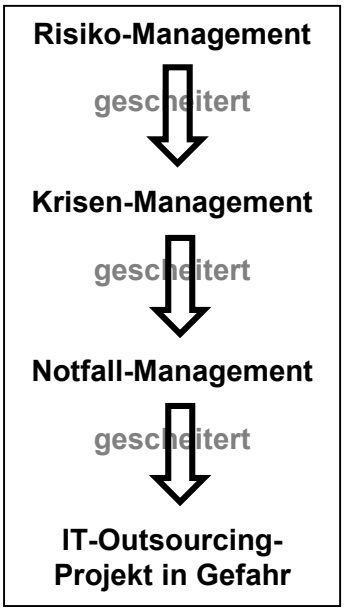
Im Gegensatz zum Risiko-Management ist das Krisen Management reaktiv. Es kommt erst dann zum Einsatz, wenn ein Problem bereits aufgetreten ist. Das Krisen-Management gewinnt also zu dem Zeitpunkt an Bedeutung, ab dem das Risiko-Management gescheitert ist und ein Risiko tatsächlich aufgetreten ist (vgl. Versteegen 2003, S. 62). Das Scheitern des Risiko-Managements kann dabei mehrere Gründe haben. So kann das eingetretene Risiko nicht vorhersehbar gewesen sein oder das Risiko war zwar vorhersehbar, wurde allerdings in der Eintrittswahrscheinlichkeit unterschätzt. Ein weiterer Grund könnte sein, dass die möglichen Auswirkungen zu gering eingestuft wurden oder in der aufgetretenen Form nicht vorhersehbar waren. Die Schwere des Risikos wurde also unterschätzt (vgl. Versteegen 2003, S. 63).

Bevor das Risiko-Management zum Einsatz kommt, müssen allerdings einige Bedingungen erfüllt sein. Zieht man ein IT-Outsourcing-Projekt bei dem ein Risiko aufgetreten ist als Beispiel heran, gelten folgende Bedingungen (Versteegen 2003, S. 63):

- „Der reguläre Fortschritt des Projektes ist gefährdet oder sogar ausgeschlossen.
- Auf der Ebene des Projekt-Managements kann keine Lösung mehr gefunden werden, weil die Auswirkungen des Risikos zu gravierend sind.
- Um reagieren zu können, müssen die Auswirkungen des Risikos bewusst sein und möglichst mit dem entsprechenden Zahlenmaterial versehen sein.“

Möchte man die Begriffe Risiko und Krise voneinander abgrenzen, dann kann man eine Krise als die erste Eskalationsstufe eines unterschätzten oder nicht erkannten Risikos betrachten, das beispielsweise innerhalb eines IT-Outsourcing-Projektes eingetreten ist.

Aufgabe des Krisen-Managements[33] ist es, eine Krise zu lösen. Es sollen also die Auswirkungen des eingetretenen Risikos in einem erträglichen Rahmen gehalten werden. Konnte auch das Krisen-Management nicht weiterhelfen, kommt das Notfall-Management zum Zug.



Ähnlich wie das Krisen-Management, das dann in Kraft tritt, wenn das Risiko-Management gescheitert ist, gewinnt das Notfall-Management dann an Bedeutung, wenn wiederum das Krisen-Management gescheitert ist. Die unterschiedlichen Eskalationsstufen führen also vom Risiko hin zur Krise und schließlich zum Notfall. Ein Notfall bildet damit die zweite Eskalationsstufe eines eingetretenen Risikos (vgl. Versteegen 2003, S. 64) Die aus einem eingetretenen Risiko resultierende Krise konnte also nicht bewältigt werden. Kann auch der Notfall nicht gelöst werden ist das gesamte IT-Outsourcing-Projekt in Gefahr.

Abbildung 17: Risiko-Management, Krisen-Management und Notfall-Management (Quelle: Eigene Darstellung)

Allein durch das Risiko-Management kann trotz allem kein Projekt in einem sicheren Umfeld gehalten werden, da es z.B. auch Risiken gibt, die nicht vorhersehbar sind. Mit Hilfe des Risiko-Managements kann zwar eine Risikoreduktion stattfinden. Ein Restrisiko bleibt dennoch vorhanden. Aus diesem Grund ist die rechtzeitige Entwicklung von Notfallplänen notwendig.

[33] Zum Krisen-Management soll vertiefend auf Neubauer (2003) verwiesen werden.

5 Entwicklung eines Leitfadens für ein Risiko-Management beim Outsourcing von IT

5.1 Entwicklung des Leitfadens

In den vorangegangenen Kapiteln wurde ein allgemeiner Überblick über das Risiko-Management gegeben und auf ausgewählte Konzepte, wie das IT-Risiko-Management, eingegangen. Im Folgenden soll nun erläutert werden, wie das Risiko-Management bei einem IT-Outsourcing-Projekt realisiert und durchgeführt werden kann. Dies wird in Form eines Leitfadens geschehen. Ziel des Leitfadens wird dabei sein, eine mögliche Vorgehensweise aufzuzeigen, wie das Risiko-Management in IT-Outsourcing-Projekten eingegliedert und durchgeführt werden kann. Der Leitfaden wird deswegen zum einen auf die Rahmenbedingungen für ein Risiko-Management bei IT-Outsourcing-Projekten eingehen und zum anderen eine mögliche Vorgehensweise für ein Risiko-Management bei IT-Outsourcing-Projekten aufzeigen. Der Leitfaden wird eine allgemeine Form und Gültigkeit haben, da jedes IT-Outsourcing-Projekt verschieden ist und dementsprechend andere Risiken aufweist.

Mittelpunkt eines jeden Risiko-Managements ist der Risiko-Management-Prozess. Aus diesem Grund soll dieser auch im Falle des Leitfadens den Mittelpunkt bilden.

Zur Entwicklung des Leitfadens wurden das Risiko-Management bei allgemeinen IT-Projekten und das IT-Risiko-Management herangezogen. Diese Vorgehensweise hat zwei Gründe. Zum einen sind sie von allen Risiko-Management-Konzepten der IT-Outsourcing-Thematik am naheliegendsten und zum anderen können sie für das Risiko-Management von IT-Outsourcing-Projekten unterstützend herangezogen werden.

5.2 Struktur des Leitfadens

Der Leitfaden wird im Folgenden aus zwei Teilen bestehen. Thema des ersten Teils werden die Rahmenbedingungen sein, die für ein Risiko-Management beim Outsourcing der IT gebraucht werden. Das eigentliche Risiko-Management wird Schwerpunkt des zweiten Teils sein und aus diesem Grund den Risiko-Management-Prozess eines IT-Outsourcing-Projekts beinhalten. Begonnen wird der Leitfaden mit den Rahmenbedingungen. Grund für diese Vorgehensweise ist, dass für ein effizientes Risiko-Management zunächst die Rahmenbedingungen überblickt und falls nötig geschaffen werden müssen.

Die beiden Teile können zusammen in einem Leitfaden dargestellt werden. Von dieser Vorgehensweise wird aber im Folgenden kein Gebrauch gemacht. Zur Reduktion von Komplexität und für eine bessere Übersichtlichkeit, sollen die beiden Teile in separaten Leitfäden erläutert werden. Es wird also ein Leitfaden für die Rahmenbedingungen und einer für den Risiko-Management-Prozess entwickelt. Diese beiden Teile sind dennoch nicht unabhängig voneinander zu betrachten, sondern bauen aufeinander auf.

Inhaltlich enthält der Leitfaden für die Rahmenbedingungen Klärungen, die im Vorfeld getätigt werden müssen und Maßnahmen, die zur Konzeption und Implementierung des Risiko-Managements beim IT-Outsourcing getätigt werden müssen.

Inhalt des zweiten Leitfadens werden dann vor allem die einzelnen Prozessphasen des Risiko-Managements sein, also die Vorgänge der Identifikation, der Bewertung, der Steuerung und der Kontrolle von IT-Outsourcing-Risiken.

Jeder Leitfaden wird eine Reihe von Punkten enthalten, die durchgeführt oder berücksichtigt werden müssen. Man kann dabei auch von Schritten sprechen, die zu einer wirkungsvollen Begleitung eines IT-Outsourcing-Projekts durch das Risiko-Management getätigt werden sollten.

5.3 Leitfaden

5.3.1 Leitfaden zur Schaffung der Rahmenbedingungen für ein erfolgreiches Risiko-Management beim Outsourcing von IT

1. Klärung der Rahmenbedingungen des Risiko-Managements

Bevor ein Risiko-Management für ein IT-Outsourcing-Projekt entwickelt wird, empfiehlt es sich, zunächst zu untersuchen, welche Rahmenbedingungen einem dabei begegnen. Zu klären sind dabei die Fragestellungen,

- ob ein unternehmensweites Risiko-Management vorhanden ist,
- ob ein IT-Risiko-Management vorhanden ist,
- ob das Unternehmen generell Erfahrung im Umgang mit Risiken hat und
- ob eine Risikokultur vorhanden ist.

Je nachdem, wie die Antworten auf diese Fragestellungen lauten, hat das unterschiedliche Konsequenzen für das Risiko-Management von IT-Outsourcing-Projekten. Ist ein unternehmensweites integriertes Risiko-Management vorhanden, so ist das Risiko-Management von IT-Outsourcing-Projekten Bestandteil des unternehmensweiten Risiko-Managements.

Hat ein Unternehmen bereits Erfahrungen im Umgang mit Risiken gesammelt, kann auf diese zur Unterstützung für eine Entwicklung eines Risiko-Managements bei IT-Outsourcing-Projekten zurückgegriffen werden.

Hat ein Unternehmen keine oder nur wenig Erfahrung im Umgang mit Risiken, ist die Realisierung eines Risiko-Managements bei IT-Outsourcing-Projekten schwieriger, weil auf keine internen Erfahrungen zurückgegriffen werden kann und davon auszugehen ist, dass keine Risikokultur vorhanden ist.

Das Vorhandensein einer Risikokultur ist dabei ein wichtiger Faktor, da der Erfolg des Risiko-Managements in besonderem Maße davon beeinflusst wird, wie es von den beteiligten Personen gelebt und umgesetzt wird. In einem für Risiken sensibilisierten Unternehmen kann es also besser realisiert werden. Ist keine Risikokultur vorhanden, sollte zumindest projektintern die Bereitschaft zur Wahrnehmung von Risiken durch die Projektmitglieder, die Sensibilisierung der Mitarbeiter und die Kommunikation der Risiken gefördert werden.

Auch die Rahmenbedingungen, die durch das Management vorgegeben werden, sind dabei zu klären. Dazu gehören z.B. die Einstellung zu Risiken, Zielsetzungen im Umgang mit Risiken oder die Einbringung einer Nachweispflicht durch die Geschäftsleitung.

2. Heranziehen des IT-Risiko-Managements

Ist ein IT-Risiko-Management in einem Unternehmen vorhanden, empfiehlt es sich dieses für das IT-Outsourcing-Projekt heranzuziehen. Dies hat zwei Gründe. Zum einen ist durch ein Outsourcing der IT das IT-Risiko-Management unmittelbar betroffen und zum anderen kann es das Risiko-Management vom Outsourcing-Projekt unterstützen.

Vor allem zur erfolgreichen Bewältigung von IT-Risiken kann von Erfahrungen (Vorgehensweisen, Auswahl der Hilfsmittel und Risikostrategie etc.) des IT-Risiko-Managements profitiert werden.

3. Benennung eines Risikoverantwortlichen

Je nach Größe und Komplexität des IT-Outsourcing-Projekts sind unterschiedliche Rollen erforderlich. Wichtig ist, dass der gesamte Prozess des Risiko-Managements unter der Koordination eines Risikoverantwortlichen steht (Kirchner 2002, S. 21). Diese Aufgabe kann bei kleinen Projekten vom Projektleiter[34] übernommen werden. Bei größeren und komplexeren Projekten empfiehlt sich diese Aufgabe an einen sogenannten Risk Officer zu übertragen.

Unabhängig davon, wer die Risikoverantwortung übernimmt, sollte der Verantwortliche Erfahrung im Umgang mit Risiken und mit den Hilfsmitteln des Risiko-Managements haben.

---

[34] Ein Management-Leitfaden zur Führung von Projekten ist bei Heilmann/Etzel/Richter (2003) zu finden.

Gründe dafür sind, dass es ein Erfahrungspotenzial erfordert, um beispielsweise Risiken hinsichtlich ihrer Eintrittswahrscheinlichkeit und Auswirkungen einschätzen zu können oder die richtige Risikostrategie zu wählen.

Im Bedarfsfall sollte ein externer Berater herangezogen werden.

4. Etablierung des Risiko-Management-Prozesses in die Projektorganisation

Sind die Rahmenbedingungen des Risiko-Managements geklärt und ein Risikoverantwortlicher ernannt, gilt es, das Risiko-Management in die Projekt-organisation einzuführen. Vor allem bei Unternehmen mit wenig Erfahrung im Risiko-Management empfiehlt sich, die Einführung desselben in ein IT-Outsourcing-Projekt selbst als Projekt durchzuführen. Dieser Vorgang besteht aus den drei Phasen Start, Installation und Verbesserung (vgl. Wallmüller 2004, S. 193). Diese Schrittweise Einführung ist deshalb sinnvoll, weil dadurch eine Anpassung des Risiko-Management-Prozesses und seiner Hilfsmittel an die Gegebenheiten des IT-Outsourcing-Projekts bewirkt werden kann. Auch können sich die beteiligten Personen den geplanten Veränderungen so schrittweise anpassen. Vor allem bei Unternehmen mit wenig Erfahrung im Umgang mit Risiken ist diese Vorgehensweise sinnvoll.

Der erste Aufgabenbereich bei der Implementierung des Risiko-Managements ist die Startphase. In dieser Phase werden die Grundlagen für die erfolgreiche Einführung geschaffen. Zu den Aufgaben dieser Phase gehören die Schaffung eines ersten Verständnisses für das Risiko-Management (z.B. durch Informationsveranstaltungen, Vertrautmachen mit allen Hilfsmitteln etc.), die Bereitstellung von genügend Ressourcen und die Etablierung einer Infrastruktur (z.B. Risk Officer etc.) (vgl. Wallmüller 2004, S. 193f).

Die zweite Phase ist die Installationsphase. Das Projektteam versucht in dieser Phase bereits das Risiko-Management in seiner Umgebung zu praktizieren. Das Risiko-Management wird also in die gängigen Praktiken des Projekt-Managements integriert. Auch findet eine Anpassung des Risiko-Management-Prozesses und seiner Hilfsmittel an die Projektumgebung statt. Somit können Grundpraktiken, wie die Identifikation von neuen Risiken eingeführt werden. Das Wesentliche dieser Phase ist, dass die Aufgaben des Risiko-Managements schnell zur Routine im Projekt werden. Das Risiko-Management soll also schnell zur Anwendung kommen (vgl. Wallmüller 2004, S.194).

Die dritte Phase ist schließlich die Verbesserungsphase. Nach dieser Phase sollte das Risiko-Management vollständig im Projekt-Management integriert sein. Ziel dieser Phase ist deshalb der effiziente und kontinuierliche Betrieb des Risiko-Managements. Aus diesem Grund ist auch die ständige Verbesserung Gegenstand dieser Phase. Zu diesem Zweck sollten periodische Überprüfungen des Prozesses und der Arbeitsweisen durchgeführt werden. Auch kann der Einsatz von Checklisten hilfreich sein (vgl. Wallmüller 2004, S.194).

5. Einbindung der Projektmitglieder

Ein Risiko-Management ist nur durch die Einbeziehung aller beteiligten Personen möglich. Für das Funktionieren des Risiko-Managements in IT-Outsourcing-Projekten sollte man deshalb alle Projektmitglieder zur Mitarbeit heranziehen. Jedes Mitglied hat unterschiedliche Blickwinkel und Erfahrungswerte. Zu einem effizienten Risiko-Management führt also erst die Zusammenführung verschiedener Informationen.

6. Kontinuierliche Information und Kommunikation aller Beteiligten

Es empfiehlt sich schon im Vorfeld alle Verantwortlichen und Beteiligten über Risikostruktur und –stand, sowie Zielverfolgung, zu informieren, um eine Mitarbeit aller Beteiligten zu fördern. Eine offene Informationspolitik zahlt sich in der Regel langfristig aus. Informiert werden kann dabei beispielsweise durch Informationsveranstaltungen für Interessierte und Beteiligte. Solche Maßnahmen können auch die Akzeptanz des Risiko-Managements bei den Beteiligten fördern.

7. Weitergabe der Risikoinformationen an das unternehmensweite Risiko-Management

Das Risiko-Management des IT-Outsourcing-Projekts sollte zusätzlich, falls ein unternehmensweites Risiko-Management vorhanden ist, auch an dieses in regelmäßigen Abständen Risikoinformationen zukommen lassen. Dort können sie gesammelt, aggregiert und für unternehmensweite Auswertungen zur Verfügung gestellt werden.

5.3.2 Leitfaden zum Risiko-Management beim Outsourcing von IT

1. Anwendung des Risiko-Management-Prozesses für allen Phasen des IT-Outsourcings

Bei der Systematisierung der Risiken des IT-Outsourcings können zwei Phasenabschnitte der Risikobetrachtung unterschieden werden. Zum einen die Projektphasen, die den Outsourcing-Prozess an sich zum Mittelpunkt der Risikoentstehung haben, und zum anderen die Betriebsphase, welche die Risiken, die nach dem IT-Outsourcing für Unternehmen entstehen, zum Betrachtungsgegenstand hat. Vereinfacht ausgedrückt, bedeutet diese Aufteilung, dass es Risiken während des IT-Outsourcing-Projekts gibt und Risiken, die nach der Realisierung dieses Vorhabens, und damit durch das IT-Outsourcing selbst entstehen. Ein Risiko-Management für ein IT-Outsourcing-Projekt sollte beides berücksichtigen. Aus diesem Grund muss das Risiko-Management kontinuierlich über den gesamten Lebenszyklus des Outsourcing-Projekts durchgeführt werden und damit jede Phase des IT-Outsourcings berücksichtigen.

Damit die Risiken von jeder Phase des IT-Outsourcing-Projekts berücksichtigt werden können, empfiehlt sich deshalb die Einführung des Risiko-Managements bereits in der Vorbereitungsphase.

2. Identifikation der Risiken bei einem IT-Outsourcing-Projekt

Der erste wesentliche Schritt bei allen Risiko-Management-Prozessen beginnt mit der Identifikation der Risiken. Dies gilt auch beim Risiko-Management von IT-Outsourcing-Projekten. Ziel der Identifikation sollte dabei sein, möglichst alle Risiken des Projekts zu erkennen. Wichtige Kriterien sind deshalb die Vollständigkeit und Aktualität der Risikoerfassung.

Folgende Tätigkeiten tragen zur Erleichterung der Identifikation bei (vgl. Wallmüller 2004, S. 133):

- Ermutigung des gesamten Projektteams, Informationen über vorhandene Risiken zu sammeln.
- Rechtzeitige Identifizierung der Risiken des IT-Outsourcings, um noch die Möglichkeit zu haben Maßnahmen zu ergreifen. Projektüberraschungen können so vermieden werden.
- Formulierung der Risiken in verständlicher Form.
- Kommunikation der Risiken an all jene, die sie auflösen können.

3. Vorgehensweise zur Risikoidentifikation

Ziel der Risikoidentifikation ist es, so viele Risiken wie möglich zu erkennen. Dazu empfiehlt sich die Umsetzung in einzelnen Schritten zu vollziehen.

Der erste Schritt ist das Durchführen eines Risiko-Assessments (vgl. Wallmüller 2004, S. 134). Dieser ist eine unsystematische Vorgehensweise, die dazu dient so viele potenzielle Risiken wie möglich heranzutragen. Er ist mit einem Brainstorming vergleichbar.

Der zweite Schritt ist die systematische Risikoidentifikation (vgl. Wallmüller 2004, S. 134). In diesem Schritt sollte systematisch nach Risiken gesucht werden. Dazu können Hilfsmittel[35] genutzt und mögliche Risikoquellen untersucht werden. Der erste und der zweite Schritt dienen dem Sammeln von Risikopotenzialen und können auch als Risikoinventur bezeichnet werden.

Hat man im Idealfall alle Risiken gesammelt, gilt es in einem dritten Schritt Übersicht über die gesammelten Risiken zu bekommen. Dazu sollten die Risiken beschrieben, auf Abhängigkeiten untersucht und in Risikokategorien eingeteilt werden.

---

[35] Mögliche Hilfsmittel wurden in Kapitel 4.3.1 beschrieben. Werden aber für den Leitfaden im nächsten Punkt (3) noch einmal aufgegriffen.

Zur Erstellung von Risikokategorien können im Falle des Vorhandenseins eines unternehmensweiten Risiko-Managements dessen Risikokategorien herangezogen werden. Auf Grund des Umfangs an unterschiedlichen Risiken bei einem IT-Outsourcing-Projekt sollten jedoch eigene Kategorien[36] entwickelt werden. Mögliche Risikokategorien sind die Aufteilung der Risiken in Projektrisiken, menschliche Risiken, Risiken durch den Outsourcing-Provider, IT-Risiken und Risiken für das Betriebs-Management.

Für die Identifizierung der Risiken stehen unterschiedliche elektronische Hilfsmittel zur Verfügung. So können durch Exceltabellen Risikolisten erstellt werden. In diesen können alle erkannten Risiken gesammelt werden. Diese Listen sollten über den weiteren Projektverlauf kontinuierlich gepflegt und weiterentwickelt werden.

Weiter kann eine Risikoabhängigkeitsliste erstellt werden. In dieser Liste wird jedes Risiko darauf untersucht, ob es von einem anderen in irgendeiner Weise beeinflusst wird. Sie ist dazu mit der Risikoliste zu verknüpfen und vereinfacht das Auffinden potenzieller neu eintretender Risiken und wird deshalb besonders beim Monitoring benötigt (vgl. Versteegen 2003, S. 91).

Abgesehen von Standardsoftware können auch professionelle Werkzeuge genutzt werden, wie das Telelogic Doors, das ein Werkzeug für das Anforderungsmanagement ist, aber auch im Risiko-Management eingesetzt werden kann (vgl. Versteegen 2003, S. 93).

4. Nutzung von Hilfsmitteln für die Identifikation von Risiken

Zur Erkennung der Risiken sollten passende Hilfsmittel verwendet werden. Dazu gehören Checklisten, Interviews mit Fragebogen, Meetings und moderierte Workshops.

Die genannten Hilfsmittel können auch kombiniert werden. In der Praxis hat sich die Kombination aus moderierten Workshops und dem Einsatz von Checklisten als wirksames Vorgehen herausgestellt (vgl. Wallmüller 2004, S.136).

Checklisten sind ein leicht zu benutzender, systematischer Weg zur Erkennung von Risiken. Man kann dabei standardisierte Checklisten verwenden oder neue entwickeln. Standardisierte Checklisten sind dabei in der Regel nicht komplett situationsgerecht.

Moderierte Workshops wiederum ermöglichen es Risiken umfassend und situationsgerecht zu finden. Zur Erkennung von Risiken können in diesem Zusammenhang Brainstormings, Nachdenken oder Modellierung bzw. Simulation verwendet werden.

---

[36] Ein ausführliches Beispiel für eine mögliche Kategorisierung der Risiken des IT-Outsourcing ist in Kapitel 3 zu finden.

5. Nutzung von internen Quellen für die Identifikation von Risiken

Quellen der möglichen Risikoentstehung erhöhen die Wahrscheinlichkeit für die Identifikation von Risiken und sollten deshalb untersucht werden. Bei einem IT-Outsourcing-Projekt können dabei Quellen herangezogen werden, die sich aus dem Projekt-Management oder der Outsourcing-Thematik ergeben.

Quellen aus dem Projekt-Management, die herangezogen werden können, sind:

- Der Projektzeitplan
- Der Projekt-Management-Plan
- Der Projektstrukturplan
- Vorgaben für Budgets
- Arbeitspaketbeschreibungen
- Ressourcenpläne

Quellen, die sich aus der Outsourcing-Thematik ergeben, sind:

- Der Prozess der Partnerwahl
- Der Outsourcing-Vertrag
- Der IT-Dienstleister
- Risikovorsorgemaßnahmen

6. Nutzung von externen Informationsquellen zur Identifikation von Risiken

Zwar ist jedes IT-Outsourcing-Projekt individuell und weist somit unterschiedliche Risiken auf, es gibt jedoch Risiken, die bei allen IT-Outsourcing-Projekten auftauchen. Zur Identifikation können deshalb auch Informationen (speziell Risikoinformationen) von anderen Unternehmen herangezogen werden. Auch Fachbücher können hilfreich sein.

Zu den Risiken, die jedes IT-Outsourcing-Projekt aufweist, gehören:

- Der Risikofaktor Projekt-Management (Verfügbarkeit von Ressourcen, Plausibilität der Meilensteine etc.)
- Der Risikofaktor IT-Outsourcing (Gefahr der falschen Partnerwahl, ungenaue Definition der Outsourcing-Leistung, unzulängliche vertragliche Regelungen etc.)
- Der Risikofaktor Mensch (Gefahr der Störung des Betriebsklimas, Nicht-Akzeptierung der neuen Situation, Widerstand im auslagernden Unternehmen etc.)
- Der Risikofaktor Outsourcing-Provider (Gefahr einer langfristigen und starken Abhängigkeit, Gefahr einer schlechten Leistungserbringung etc.)
- Der Risikofaktor IT (Gefahr des Ausfalls der IT-Systeme, unzureichende Zutrittskontrollen, schlechte oder fehlende Authentikation)

- Der Risikofaktor Betriebs-Management (Verlust von Know-how, zusätzliche Kosten, Verlust von Entscheidungsspielräumen etc.)

7. Bewertung der Risiken bei einem IT-Outsourcing-Projekt

Der zweite Schritt nach der Risikoidentifikation ist bei allen Risiko-Management-Prozessen die Bewertung bzw. Analyse der Risiken.

Zu diesem Zweck ist der Kontext der Risiken zu klären und zu vertiefen. Es gilt, das Ausmaß der Risikodarlegung und die Risiken mit der höchsten Priorität zu bestimmen. Auch ist es wichtig einen Zeitrahmen festzulegen, in dem Maßnahmen für einzelne Risiken zu ergreifen sind.

Die Aktivitäten, die in diesem Prozessschritt gemacht werden müssen, sind deshalb (vgl. Wallmüller 2004, S.138):

- Bewertung der Risiken durch die Attribute Wahrscheinlichkeit des Eintretens, Auswirkungen des Eintretens und Zeitspanne, in der Maßnahmen ergriffen werden sollten,
- Filterung und Priorisierung der Risiken,
- Bestimmen der Ursachen der Risiken,
- Bildung einer Top N-Liste der Risiken.

Zur Bewertung der Risiken können das Risikoerfassungsformular und die Risikomatrix als Hilfsmittel genutzt werden.

8. Beurteilung der Eintrittswahrscheinlichkeiten und der Auswirkungen von Risiken

Die Beurteilung der Eintrittswahrscheinlichkeit sollte von einem Team durchgeführt werden, da die Einschätzung subjektiv ist[37]. Bei einem IT-Outsourcing-Projekt bietet es sich an, für diese Einschätzungen das Projektteam heranzuziehen. Die Projektmitglieder sollten dabei ihre subjektive Meinung der Eintrittswahrscheinlichkeit eines konkreten Risikos abgeben. Dies kann in Form eines Konsensverfahrens mit einer festgelegten Punkteskala, die z.B. einen Wertebereich von 1 bis 10 hat, stattfinden. Mit Hilfe von mathematischen Verfahren können die Einschätzungen zu einer einzigen Risikomaßzahl aggregiert werden. Die Gefahr einer Fehleinschätzung kann so verkleinert werden (vgl. Versteegen 2003, S.102).

---

[37] Eine Bewertung der Risiken – auch der Risiken, die in der Regel in jedem IT-Outsourcing-Projekt zu finden sind - kann deshalb im Rahmen des Leitfadens nicht stattfinden. Auch in der verwendeten Literatur waren keine Beispiele für Bewertungen von Risiken im Rahmen des IT-Outsourcings zu finden.

Anschließend können die Risiken in Wahrscheinlichkeitsklassen eingeteilt werden. Folgende Risikowahrscheinlichkeitsklassen sind sinnvoll (vgl. Versteegen 2004, S. 136):

- RWK 1: Das Eintreten des Risikos ist durchaus wahrscheinlich.
- RWK 2: Das Eintreten des Risikos ist möglich.
- RWK 3: Das Eintreten des Risikos ist nur unter bestimmten Bedingungen möglich.
- RWK 4: Das Eintreten des Risikos ist eher unwahrscheinlich.
- RWK 5: Das Eintreten des Risikos ist nahezu ausgeschlossen.

Eine ähnliche Vorgehensweise sollte auch zur Bewertung der Schadenshöhe, also der Auswirkungen beim Eintreten von Risiken, vorgenommen werden. Versteegen empfiehlt dazu eine Skala von nur drei Punkten festzulegen, von eins (niedriger Schaden) bis drei (hoher Schaden). Zusätzlich sollten zur Ermittlung der Schadenshöhe die Parameter Zeit, Kosten und Funktionalität gesondert betrachtet werden (vgl. Versteegen 2004, S. 108):

Wichtig ist, dass die Skalen für alle Teammitglieder verbindlich festgelegt und entsprechend kommuniziert werden.

9. Berücksichtigung der Wechselbeziehungen von Risiken

Abgesehen von der Eintrittswahrscheinlichkeit und der Schadenshöhe sollten bei der Bewertung der Risiken des IT-Outsourcing-Projekts auch die Abhängigkeiten untersucht werden. So kann ein Risiko sowohl in Eintrittswahrscheinlichkeit als auch in Schadenshöhe niedrig eingestuft sein, aber beim Eintreten weitere Risiken mit hohen Konsequenzen beeinflussen. Solche Wechselbeziehungen sollten berücksichtigt werden.

10. Unterscheidung von Primär- und Sekundärrisiken

Wichtig bei der Bewertung von Risiken ist die Definition von Primär- und Sekundärrisiken. Bei der Fülle an Risiken, die mit einem IT-Outsourcing-Projekt verbunden sind, können nicht alle Risiken mit der gleichen Sorgfalt und sämtlichen Planungsmaßnahmen, wie Verhinderung, Verringerung, Schadensbegrenzung und Notfallplanung behandelt werden. Zur Priorisierung der Risiken sollte man die Ergebnisse aus der Einschätzung der Eintrittswahrscheinlichkeit und der möglichen Auswirkungen heranziehen, sowie die möglichen Wechselbeziehungen berücksichtigen.

11. Steuerung der Risiken bei einem IT-Outsourcing-Projekt

Nach der Risikobewertung ist der darauffolgende Schritt bei einem Risiko-Management-Prozess immer die Risikosteuerung. Hat man die Risiken des IT-Outsourcing-Projekts erkannt, analysiert und bewertet, gilt es diese in einem nächsten Schritt zu steuern.

Im Rahmen der Risikosteuerung sollen die Risiken nach den Prozessschritten der Risikoidentifikation und Risikobewertung, entsprechend ihrer Risikoposition, aktiv beeinflusst werden. Ziel der Maßnahmen, die für die Steuerung getroffen werden, ist dabei eine Verringerung der Eintrittswahrscheinlichkeit und/oder eine Begrenzung der Auswirkungen beim Eintreten eines Risikos.

Zur Aufgabe der Risikosteuerung gehört es deshalb wirksame Entscheidungen in Bezug auf die Risiken und ihrer Behandlungsmaßnahmen zu treffen und diese konsequent durchzuführen. Eine effektive Risikosteuerung erfordert aus diesem Grund zum einen eine fortlaufende Bewertung der Risikobehandlungsmaßnahmen und zum anderen eine Bewertung der Qualität der Ausführung der geplanten Maßnahmen (Wallmüller 2004, S. 149).

12. Einbindung der Entscheidungsträger

Die Identifikation und Analyse der Risiken sind Aufgaben, die direkt vom Projektteam erledigt werden können. Bei Planungsmeetings zur Steuerung der Risiken sollte man auch Entscheidungsträger einladen, da das Projektteam bei der Planung von Maßnahmen in der Regel die Genehmigung zur Umsetzung braucht.

13. Festlegung von Risikostrategien

Für jedes erkannte Einzelrisiko des IT-Outsourcing-Projekts sollte im Rahmen der Risikosteuerung eine Risikostrategie festgelegt werden. Es gilt also nicht eine Gesamtstrategie für alle Risiken, da jedes Risiko mit einer eigenen Strategie bearbeitet wird. Eine Strategie kann jedoch für mehrere Einzelrisiken angewendet werden.

Übliche Risikostrategien und damit Instrumentarium zur Risikosteuerung sind die Risikovermeidung, die Risikoakzeptierung, die Risikominimierung und die Risikoübertragung.[38]

Welche Strategie für jedes einzelne Risiko angewendet wird, ergibt sich aus der Risikobewertung. Wird ein Risiko als primäres Risiko eingestuft, empfiehlt sich eine Risikovermeidung. Ist die Vermeidung nicht möglich, sollte zumindest das Risiko minimiert werden. Ist ein Risiko sekundär, kann auch eine Risikoakzeptierung genügen.

[38] Vgl. Kapitel 4.3.3

14. Nutzung der Möglichkeiten des IT-Outsourcings zur Risikosteuerung

Zu einer Steuerung der Risiken ist es sinnvoll, die Möglichkeiten zur Vermeidung bzw. Minimierung von Risiken, die dem IT-Outsourcing-Projekt zur Verfügung stehen, zu nutzen. Dies gilt vor allem für Risiken, die bei allen IT-Outsourcing-Projekten vorkommen.

Das IT-Outsourcing hat u.a. folgende Möglichkeiten zur Risikosteuerung:

- Besondere Aufmerksamkeit beim Prozess der Partnerwahl
- Steuerung durch den Outsourcing-Vertrag
- Definition von Service Level Agreements (SLAs)
- Erstellung eines IT-Sicherheitskonzepts
- Information und Kommunikation der beteiligten Einheiten

15. Notwendigkeit einer besonderen Aufmerksamkeit bei der Partnerwahl

Durch eine besondere Aufmerksamkeit bei der Partnerwahl kann der Risikofaktor Outsourcing-Provider und die damit verbundenen Risiken verringert werden. Das Risiko von Fehltritten kann nur durch eine detaillierte und sorgfältige Partnersuche[39] minimiert werden. Aufgabe des Risiko-Managements ist es deshalb auf die Qualität der Suche zu achten, um die Outsourcing-Erwartungshaltung im Hinblick auf den Outsourcing-Provider größtmöglich zu erfüllen. Es ist darauf zu achten, dass die Wahl für einen Outsourcing-Dienstleister nicht allein aus Gründen der Preisgünstigkeit getroffen wird. Auch das Leistungsangebot und die Verhältnisse des Providers (Rechtsform, Organisation, wirtschaftliche Lage, Leistungsfähigkeit) sind zu klären.

16. Steuerung durch den Outsourcing-Vertrag

Auch der Outsourcing-Vertrag bietet die Möglichkeit zur Reduzierung der Risiken, die durch einen Outsourcing-Provider entstehen. Der Outsourcing-Provider verpflichtet sich durch diesen Vertrag zur Leistungserbringung an den Outsourcinggeber. Eine detaillierte vertragliche Regelung im vorhinein ist deshalb wichtig. Darüber hinaus dient sie zur Übersicht für beide Vertragspartner, da durch den Vertrag Klarheit geschaffen werden kann, welche Voraussetzungen erfüllt werden müssen, um die Zusammenarbeit zum Erfolg zu führen. Es ist sinnvoll die Thematik der Informationssicherheit in den Vertrag miteinzubauen. Die Sicherheit von Daten und Informationen wird so auf beiden Seiten verpflichtend. IT-Risiken können so verringert werden.

[39] vgl. Kapitel 2.4.2

Der Vertrag kann bei schlechter Ausarbeitung zum Risikofaktor werden, bei guter aber auch zur Risikosteuerung. Die Vertragsphase sollte deshalb unbedingt vom Risiko-Management und gegebenenfalls von Spezialisten zur Vertragsgestaltung begleitet werden.

17. Nutzung der Service Level Agreements

Effektives Mittel zur Risikosteuerung von Risiken im Hinblick auf den Outsourcing-Provider sind auch die Service Level Agreements (SLAs) als Ergänzung zu den vertraglichen Regelungen. Die Leistungserbringung kann durch sie unterstützend gewährleistet werden, da Verantwortlichkeiten, Leistungen, Qualitäten und spezifische Rahmenbedingungen festgelegt werden. Der Grad der Leistungserfüllung kann also mit Hilfe der SLAs als Messinstrument erkannt werden.

Zusätzlich bieten SLAs die Möglichkeit zur Definition von Vertragsstrafen, falls die Leistungen des Providers nicht den vertraglichen Abmachungen entsprechen. SLAs können so als Druckmittel verwendet werden.

Auch die SLAs sind Risikofaktor und Möglichkeit zur Risikosteuerung zugleich und sollten bei der Formulierung deshalb vom Risiko-Management begleitet werden, um später die Möglichkeit zur Risikosteuerung zu erhalten. Einen Risikofaktor bilden die SLAs dann, wenn sie zu ungenau formuliert werden und dadurch Interpretationsspielräume im Hinblick auf die Leistungserbringung eröffnen. Werden sie dagegen wirkungsvoll formuliert, dienen sie nicht nur als Instrument zur Risikosteuerung, sondern können auch als vertrauensbildende Maßnahme zwischen den beiden Outsourcingpartnern eingesetzt werden und so eine Basis des gemeinsamen Handelns schaffen.

18. Erstellung eines IT-Sicherheitskonzepts zur Steuerung der IT-Risiken

Um IT-Risiken vorzubeugen, sollte ein IT-Sicherheitskonzept existieren. Dieses enthält Maßnahmen zum Datenschutz und zur Datensicherheit. IT-Risiken können dadurch gesteuert werden. Das IT-Sicherheitskonzept sollte dabei im Verlauf des Projekts stetig weiterentwickelt und aktualisiert werden, da zu Beginn einer Outsourcing-Partnerschaft nicht alle technischen und organisatorischen Details bekannt sind (vgl. http://www.bsi.de/gshb/deutsch/menue.htm). [40]

[40] Zum Thema Sicherheit und Sicherheitsmanagement soll vertiefend auf Edelbacher/Reither/Preining (2000) verwiesen werden. Eine Anleitung zur Erstellung eines IT-Sicherheitskonzepts ist im IT-Grundschutzhandbuch (http://www.bsi.de/gshb/deutsch/menue.htm) zu finden

19. Information und Kommunikation aller beteiligten Einheiten

Eine professionelle Kommunikation sollte ebenfalls zur Risikosteuerung genutzt werden. Vor allem während der Projektphasen können menschliche Risiken dadurch gesteuert werden.

Wird ein Outsourcing-Projekt angekündigt, schafft das zunächst bei allen Betroffenen und deren Umfeld Verunsicherung, vor allem in Bezug auf ihre beruflichen Rahmenbedingungen. Durch diese Verunsicherung kann es zu Risiken (schlechtes Betriebsklima, innere Kündigung der Mitarbeiter, Widerstand der Mitarbeiter etc.) kommen. Eine offene und professionelle Kommunikation kann dem gezielt entgegenwirken, was bedeutet, dass die betroffenen Zielgruppen, angemessen über die neue Lösung und eventuelle Veränderungen informiert werden. Kann über die Lösungen und konkreten Veränderungen zu Beginn des Vorhabens noch nicht klar kommuniziert werden, ist zum einen darauf zu achten, dies später nachzuholen, und zum anderen, zumindest über den Prozess und den geplanten Ablauf Klarheit zu schaffen (vgl. Hodel/Berger/Risi 2004, S.117).

20. Entwicklung von Notfallplänen

Wird ein IT-Outsourcing-Projekt realisiert, ist nicht nur vom „best case“ auszugehen. Auch Schwierigkeiten und Notlagen können bei der Realisierung auftauchen. Der Fall des „worst case“, beispielsweise in Form von auftretenden Störungen, sollte in die Überlegungen und Planungen miteingebaut werden (vgl. Hodel/Berger/Risi 2004, S.154). Die Durchführung von Planungsszenarien und die Entwicklung von Notfallplänen kann dabei weiterhelfen.

Führt ein Unternehmen keine Planungsszenarien für mögliche Notfälle durch, kann das zur Gefahr werden, wenn akute Störungen auftauchen und die Lösungsmöglichkeiten erst entwickelt werden müssen.

Sind aber Notfallpläne ausreichend entwickelt, können sie zur Risikosteuerung beitragen. Vor allem beim Eintreten eines Risikos können sofort Maßnahmen ergriffen werden.

21. Überwachung der Risiken bei einem IT-Outsourcing-Projekt

Die letzte Stufe im Risiko-Management-Prozess des IT-Outsourcing-Projekts ist die Risikoüberwachung. Zu dieser Phase gehören die Tätigkeiten der laufenden Überwachung der Risiken, die Kontrolle der Wirksamkeit der Behandlungsmaßnahmen und das Erkennen von Veränderungen bei Risiken. Kontrollpläne können zu diesem Zweck erarbeitet werden.

Instrumentell kann diese Phase durch Abweichungsanalysen (Soll-Ist-Analysen) unterstützt werden. Dabei kann man sich z.B. an Limitgrenzen orientieren. Kennzahlen und Indikatoren sollten zu diesem Zweck definiert werden und Schwellen- bzw. Toleranzwerte festgesetzt werden. Werden diese Überschritten kann z.B. eine Meldung an den Risikobeauftragten veranlasst werden. In dieser Phase sollten also Risikomesskonzepte entwickelt und umgesetzt werden.

22. Berücksichtigung des Restrisikos

Der Schritt der Risikoüberwachung ist vor allem wichtig, weil trotz aller Risikomaßnahmen immer ein Restrisiko zurückbleibt, das überwacht werden sollte. Das Risiko-Management des IT-Outsourcing-Projekts sollte sich nicht nur auf die Risiken, die sich steuern lassen, beschränken, sondern alle Risikopotenziale berücksichtigen.

23. Kontinuierliche Wiederholung des Risiko-Management-Prozesses

Die internen und externen Rahmenbedingungen eines IT-Outsourcing-Projekts können sich im Projektverlauf wandeln. Dadurch kann sich auch die Risikosachlage verändern. Durch die einmalige Identifizierung und Analyse von Risiken ist deshalb lediglich der Beginn des Risiko-Management-Prozesses eingeläutet. Auch neu hinzugekommene Risiken müssen identifiziert werden. Für eine aktuelle und permanente Überprüfung der Risiken muss die Risikoidentifikation und damit der gesamte Risiko-Management-Prozess regelmäßig wiederholt werden.

24. Vollständige Dokumentation des Risiko-Management-Prozesses

Zur Überwachung der Risiken bei einem IT-Outsourcing-Projekt ist Transparenz, Übersichtlichkeit und Nachvollziehbarkeit von Ergebnissen und Maßnahmen wichtig. Zu diesem Zweck ist es sinnvoll, alle Tätigkeiten in den Phasen des Risiko-Management-Prozesses zu dokumentieren. Die Anforderungskriterien sind dabei die Vollständigkeit, die Aktualität und die Verfügbarkeit. Dies bedeutet, dass im Rahmen der Risikodokumentation eine vollständige Erfassung aller potentiellen Risiken des IT-Outsourcing-Projekts stattfinden sollte. Die einmal erfassten Informationen sollten dabei nicht als statisches Ergebnis aufgefasst werden, da bei der kontinuierlichen Wiederholung des Risiko-Management-Prozesses beispielsweise Risiken neu entdeckt werden und Maßnahmen zur Risikobehandlung verändert werden können. Auch die Dokumentation sollte deshalb kontinuierlich aktualisiert werden. Weiter sollte die Risikodokumentation unabhängig von Hierarchie, Ort und Zeit zur Verfügung gestellt werden.

6 Auswirkungen des IT-Outsourcings

Nachdem in den vorangegangenen Kapiteln die Durchführung des Risiko-Managments bei IT-Outsourcing-Projekten erläutert wurde, soll an dieser Stelle kurz darauf eingegangen werden, welche Auswirkungen ein Outsourcing der IT auf den Outsourcinggeber hat.

Das auslagernde Unternehmen bleibt von einem Outsourcing der IT nicht unbeeinflusst. Ist die IT eines Unternehmens erst einmal ausgelagert, ist diese Maßnahme schwer wieder umkehrbar. Ist der Auslagerungsprozess durchgeführt, Fehlen dem Unternehmen nämlich zunächst die Voraussetzungen diese Leistung kurzfristig wieder selbst zu erstellen. Grund dafür ist der Wissensabgang, der zur Wiedereingliederung der IT, einen Neuaufbau des Wissens erfordert (vgl. http://www.4managers.de/01-Themen/..%5C10-Inhalte%5Casp%5Coutsourcing.asp?hm=1&um=O).

Auch setzt sich ein Unternehmen je nach Umfang des Outsourcings erheblichen Umstrukturierungsmaßnahmen aus. Diese lassen sich dadurch begründen, dass durch ein auslagern von Teilen des Unternehmens, wie dem IT-Bereich, sich Änderungen in der Ablauforganisation ergeben. So wird die Verantwortung und Betreuung der IT durch ein Outsourcing auf ein externes Unternehmen übertragen, die IT ist aber oft noch vor Ort vorhanden. Dies erfordert die Entwicklung eines Konzepts, um die neue Situation zu bewältigen. Das Change Management kann dazu herangezogen werden. Es ermöglicht eine systematische und kostengünstige Vorgehensweise, um mit Änderungen umzugehen.

Werden das Technologie-Management und das IT-Risiko-Management nach dem Outsourcing der IT nicht aufrechterhalten, geht auch der Kontakt mit dem IT-Markt und der Informationstechnologie verloren. Änderungen und Entwicklungen im Hardware/Software-Bereich können dadurch vom Outsourcinggeber nicht berücksichtigt werden. Die Beratung durch den IT-Dienstleister wird nötig und gewinnt dadurch an Bedeutung. Dabei stellt sich die Frage nach der Form der Beratung (durch Workshops, in schriftlicher Form etc.).

Deutlich wird der stark angestiegene Bedarf an Kommunikation und Koordination mit dem Outsourcingnehmer. Es ist wichtig die Kommunikation zwischen Outsourcingnehmer und Outsourcinggeber aufrechtzuerhalten, da dadurch eine bessere Zusammenarbeit stattfinden kann. Zu diesem Zweck sollten auf beiden Seiten Ansprechpartner bestehen.

Weiter kann ein Outsourcing der IT Auswirkungen auf die Kunden haben (vgl. Hodel/Berger/Risi 2004, S. 198). Die IT eines Unternehmens trägt maßgeblich zur täglichen Geschäftsabwicklung bei.

Wird die tägliche Geschäftabwicklung durch schlechtere Leistungen des IT-Dienstleisters negativ beeinflusst, können unzufriedene Kunden die Konsequenz davon sein. Das Kunden-Management des Outsourcinggebers muss sich damit ebenfalls den neuen Gegebenheiten anpassen.

7 Exkurs: Gründe für das Scheitern von IT-Outsourcing-Projekten

Für viele Unternehmen ist die Möglichkeit durch das IT-Outsourcing, Teilleistungen des Betriebes an Dritte auszulagern, ein geeignetes Instrument, um Kosten einzusparen und um das Unternehmen in konjunkturellen Schwankungsphasen zu flexibilisieren. Den Unternehmen ist dabei häufig nicht bewusst, dass der Erfolg eines solchen Vorhabens maßgeblich von der Qualität und Leistung ihres Outsourcingnehmers abhängt. Zusätzlich kommen in vielen Fällen noch Schwierigkeiten bei der internen Ausgestaltung der Anforderungen an ein geeignetes Outsourcing-Risiko-Management hinzu. In den vergangenen Jahren gab es infolgedessen viele Unternehmen, die aus der Auslagerung von internen Leistungen Schäden davon getragen haben, die z.B. durch einen schlecht leistenden oder insolvent gewordenen Outsourcingnehmer resultierten. In vielen Fällen war der Erfolg des Outsourcing-Projekts durch solche Gründe zum Scheitern verurteilt.

Weitere Gründe, die Outsourcing-Projekte, wie das IT-Outsourcing, zum Scheitern führen können sind:

- **„Keine Planungsszenarien für mögliche Notfälle“ (Hodel/Berger/Risi 2004, S. 153)**

Möchte ein Unternehmen seine IT auslagern, ohne Planungsszenarien für mögliche Notfälle und Notfallpläne entwickelt zu haben, kann das beim Eintreten von Notfällen zu erheblichen Schwierigkeiten führen. Ausgehend von der Höhe des Risikos sind keine unmittelbaren Lösungswege vorhanden, sondern müssen erst entwickelt werden. Kann das Problem nicht rechtzeitig gelöst werden, kann das gesamte IT-Outsourcing-Projekt in Gefahr geraten.

- **Änderung in der Geschäftumgebung**

Im Verlauf der Vertragsdauer können viele Veränderungen in der Geschäftsumgebung eines auslagernden Unternehmens stattfinden. Dabei ist es nahezu unmöglich bei dem Tempo an Veränderungen in den Bereichen der Markt- und Technologieentwicklung, der künftigen Unternehmensstrukturen und –zusammenschlüsse - alles im Hinblick auf die Leistungserbringung durch den Outsourcingnehmer - vertraglich festzuhalten. Es kann sogar passieren, dass ein Outsourcing-Vertrag bereits veraltet ist, bevor die Verhandlungen der zukünftigen Outsourcing-Partner beendet sind. Die Vereinbarungen sollten deshalb für kontinuierliche Änderungen flexibel gestaltet sein (vgl. Sparrow 2003, S.198).

▪ Mangel an Flexibilität des Outsourcingnehmers (Hodel/Berger/Risi 2004, S. 153)

Eng verknüpft mit der Problematik von Änderungen in der Geschäftsumgebung ist die Problematik der mangelhaften Flexibilität des Outsourcingnehmers.

Im Verlauf der Outsourcing-Partnerschaft können unbekannte, neue Anforderungen entstehen, die Korrekturen bei der Leistungserbringung durch den Outsourcingnehmer erfordern. So kann es abgesehen von Änderungen im Unternehmensumfeld beispielsweise passieren, dass bei der Übernahme der Leistungserbringung durch den Outsourcingnehmer, Varianten der vertraglich festgehaltenen Leistungsanforderungen entstehen[41]. Mit solchen im Vorfeld unbekannten, neuen Anforderungen ist konstruktiv umzugehen. Dies erfordert die nötige Flexibilität durch den Outsourcingnehmer auf ungeplante und nicht definierte Änderungen zuvorkommend zu reagieren (vgl. Hodel/Berger/Risi, 2004, S. 154f). Ist der Outsourcingnehmer nicht bereit dazu, kann das zu erheblichen Konsequenzen im Hinblick auf die Leistungserbringung für den Outsourcinggeber kommen. In solchen Fällen ist das Szenario denkbar, dass der Outsourcinggeber einen Teil der Leistung trotz des Outsourcings selbst erbringen muss. Vorteile des IT-Outsourcings, wie Kostenersparnisse und Schaffung von Transparenz, gehen dabei verloren.

▪ Ungenügend ausgearbeiteter Outsourcing-Vertrag

Weiter kann der Grund für ein Scheitern eines IT-Outsourcing-Projekts ein ungenügend ausgearbeiteter Outsourcing-Vertrag sein. Der Outsourcing-Vertrag bildet die Grundlage einer Outsourcing-Beziehung und ist damit ein wichtiger Bestandteil für eine erfolgreiche Partnerschaft. Dementsprechend wirkt sich ein schlecht ausgearbeiteter Outsourcing-Vertrag negativ auf die Outsourcing-Beziehung aus.

Im Outsourcing-Vertrag werden die Leistungsvereinbarungen festgehalten, zu denen sich die beiden Partner verpflichten. Ist der Vertrag ungenügend ausgearbeitet, kann dies zu Unzulänglichkeiten und Unzufriedenheit führen. Schwierigkeiten können dabei entstehen, wenn der Vertrag z.B. zu unflexibel gestaltet ist, zu ungenau und lückenhaft formuliert ist und zu viel Spielraum für Interpretationen offen lässt und dadurch der Grad der Leistungserbringung ungenau wird.

▪ Kosten

Ungenaue kostenrechnerische Verfahren können das tatsächliche Kostenbild bei einem Outsourcing der IT verschleiern. So gibt es Kosten, die auf den ersten Blick nicht sichtbar sind, wie beispielsweise Transaktions- und Umstellungskosten. Dazu kommen Fixkosten, die auch nach einem Outsourcing der IT bestehen. So kann es zu einer Zunahme der Kosten in dem auslagernden Unternehmen kommen. In manchen Fällen kann der Kostenzuwachs in einem solchen Maß heranwachsen, dass ein Outsourcing nicht mehr von Vorteil ist (vgl. Sparrow 2003, S.203).

---

[41] Ursache dafür ist, dass viele Leistungen bei der Definition auf Annahmen beruhen. Erst bei der Leistungsübergabe an den Outsourcingnehmer kommt dann zum Vorschein, dass diese nicht (vollständig) korrekt waren.

8 Ausblick

Die Gründe heutzutage für ein IT-Outsourcing sind hauptsächlich die Konzentration auf die Kernkompetenzen und die Kostenreduzierung. Es ist abzusehen, dass sich die Gründe dafür künftig verändern werden. Neue Gegebenheiten werden zu neuen Anforderungen und damit zu neuen Gründen für ein IT-Outsourcing führen. So ist die schnelle Entwicklung im Bereich der IT bereits seit einigen Jahren aufgefallen. Es ist abzusehen, dass der IT-Markt weiterhin von Schnelllebigkeit geprägt sein wird. Dabei gibt es bereits heute viele Unternehmen, die ihre IT nicht mehr überschauen und auch die Entwicklungen im Technologiemarkt nicht überblicken. Künftig wird es noch mehr und kompliziertere IT-Produkte geben. Ein Grund, der dadurch für ein IT-Outsourcing vermehrt in den Vordergrund treten kann, ist der Zugang zu externem und spezialisiertem IT-Know-how.

Bereits heute wird das Risiko-Management als wichtiger Erfolgsfaktor bei IT-Outsourcing-Projekten angesehen. Dennoch ist der Einsatz des Risiko-Managments bei IT-Outsourcing-Projekten in der Praxis eher selten. Künftig wird seine Bedeutung wohl steigen, da die Konkurrenz auf dem Markt immer härter wird und die Anforderungen an die Unternehmen immer größer. Es wird also noch mehr als heute ein effektives Risiko-Management zur Steuerung der Risiken gebraucht werden, um den Herausforderungen gewachsen zu sein.

Dies wirft die Frage auf, ob das Risiko-Management mit den ihm heute zur Verfügung stehenden Mitteln ausreicht. So gibt es heutzutage zwar auch professionelle Tools, diese sind aber noch gering in der Anzahl und bedürfen in der Regel einer Weiterentwicklung. Auch die gesetzlichen Vorgaben sind noch sehr ungenau. Es lediglich ein Überwachungssystem zur Erkennung und Kontrolle gefordert. Wie dieses in der Praxis aussehen und wie effektiv es gestaltet sein soll, bleibt den Unternehmen selbst überlassen.

Eine Aufgabe für Wissenschaft und Wirtschaft sollte deshalb die Weiterentwicklung und Verbesserung der Möglichkeiten des Risiko-Managements sein, wie z.B. im gesetzlichen Bereich und im Bereich der professionellen Tools zum Risiko-Management.

9 Zusammenfassung

Ein Outsourcing der IT eröffnet neue Chancen für Unternehmen. Durch Auslagerung von unwesentlichen Rand- und Unterstützungsaktivitäten, wie dem IT-Betrieb, können sich Unternehmen auf ihre eigentlichen Stärken, ihre Kerngeschäftsfelder, konzentrieren. Langfristig wird Unternehmen dadurch die Möglichkeit gegeben, sich besser an die Markt- und Wettbewerbserfordernisse anzupassen und damit ihre Ertragskraft nachhaltig zu verbessern. Auch die Kostenreduzierung spielt bei Outsourcing-Überlegungen immer noch eine große Rolle. Abgesehen von den Möglichkeiten zur Kostenreduzierung und der Konzentration auf die Kerngeschäftsfelder ergeben sich durch ein Outsourcing der IT auch weitere Möglichkeiten, wie Zugang zu externem Know-how, Vermeidung von Ressourcenengpässen im IT-Bereich etc..

Mit einem IT-Outsourcing-Vorhaben sind jedoch nicht nur Chancen verbunden, sondern auch Risiken. Die Risiken, die damit verbunden sind, lassen sich in chronologische Phasenabschnitte ihrer Entstehung unterteilen. Demnach entstehen Risiken durch das Outsourcing der IT in den Projektphasen und der darauffolgenden Betriebsphase. Hinter jedem Phasenabschnitt verbergen sich eine Fülle an Risiken. Dabei ist nicht zu vergessen, dass jedes IT-Outsourcing-Projekt individuell ist und unterschiedliche Risiken aufweist.

Besonders auffällig bei der chronologischen Aufteilung der Risken ist die Wechselwirkung von Risiken, die in den Projektphasen entstehen, ihre Auswirkungen aber erst in der Betriebsphase haben. Dazu gehören die Partnerwahl und die Vertragsgestaltung. Wird in den Projektphasen eine falsche Partnerwahl getroffen, kann in der Betriebsphase eine schlechte Leistungserbringung des IT-Dienstleisters die Konsequenz sein. Auch durch einen zu ungenauen oder zu starr formulierten Vertrag in den Projektphasen kann es zu Schwierigkeiten in der Betriebsphase kommen. Der Outsourcing-Vertrag ist nämlich die Basis der Leistungserbringung durch den Outsourcingnehmer. Die Fülle an potenziellen Risiken zeigt die Notwendigkeit von Lösungsvorschlägen. Das Risiko-Management hat sich als möglicher Lösungsweg etabliert und wird heutzutage als wichtiger Erfolgsfaktor zur Realisierung eines IT-Outsourcing-Projekts gesehen.

Es dient dazu, Risiken im Vorfeld zu erkennen und zu bewältigen. Das Risiko-Management ist also proaktiv und kommt vor dem Eintreten von Risiken zum Einsatz. Zum Umgang mit den Risken eines IT-Outsourcing-Projekts kann der Risiko-Management-Prozess herangezogen werden, da er alle Aktivitäten zum praktischen und systematischen Umgang mit Risiken beschreibt. Seine Elemente sind die Identifikation, Bewertung, Steuerung und Bewertung von Risiken.

Abgesehen vom Instrumentarium des Risiko-Managments können auch Tätigkeiten, die im Rahmen des IT-Outsourcing-Projekts gemacht werden, zur Steuerung der Risiken herangezogen werden. Dazu gehören die Partnerwahl, der Outsourcing-Vertrag und die Formulierung von SLAs. Im Hinblick auf de IT-Outsourcing-Thematik spielt auch das IT-Risiko-Management eine wesentliche Rolle. Es umfasst alle Risiken, die mit dem Bereich der IT verbunden sind. Zur Bewältigung der IT-Risiken beim Outsourcing der Informationstechnologie kann es deswegen unterstützend beitragen.

Abschließend lässt sich sagen, dass zu einer erfolgreichen Realisierung von einem IT-Outsourcing-Projekt die Einbeziehung des Risiko-Managements notwendig ist. Die Notwendigkeit ergibt sich dabei durch die Fülle an potenziellen Risiken und der dadurch resultierenden Gefahr, dass diese das Projekt zum Scheitern bringen könnten. Ein systematischer Umgang mit den Risiken des IT-Outsourcings durch das Risiko-Management ist also unbedingt erforderlich.

Besonders zu beachten ist dabei, dass der Erfolg eines IT-Outsourcing-Projekts von der Zusammenarbeit mit dem Outsourcing-Provider abhängt. Eine gute Partnerwahl und vertragliche Gestaltung sind deshalb elementare Vorraussetzungen, um die Partnerschaft zum Erfolg zu führen und verdienen besondere Beachtung durch das Risiko-Management.

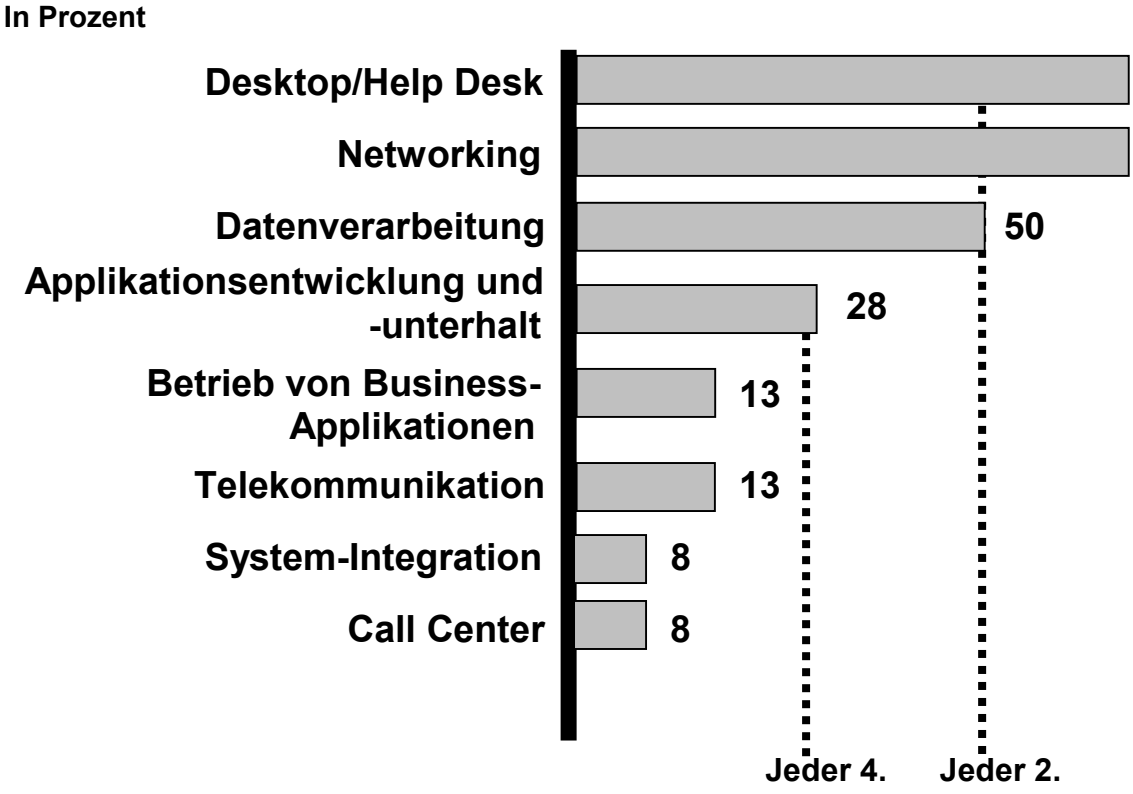
Anhang 1: Liste von professionellen Werkzeugen

Diese Liste für professionelle Werkzeuge des Risiko-Managements erhebt keinen Anspruch auf Vollständigkeit. Sie soll lediglich einen kleinen Überblick geben. Die Produktnamen sind jeweils kursiv dargestellt (Quelle: Versteegen 2003, S. 276):

- Das Produkt *RIMIS* von Antares Informationssysteme und Ernst & Young (www. Antares-is.de)
- Das Produkt *RM-EXPERT* von ASTRUM (www. Astrum.de)
- Das Produkt *CREFOsprint* von command (www.command.de)
- Das Produkt *ProKoRisk* von CORIS (www. Coris-gmbh.de)
- Das Produkt *RISK MANAGER* von CP CORPORATE PLANING (www. Corporate-planning.com)
- Das Produkt *Riskcontrol* von ifb (www.ifbag.com)
- Das Produkt *Process Risk Scout* von IDS Scheer (www.idsscheer.de)
- Das Produkt *IGW Liquiditätsplanung* vom Ingenieurbüro Gerhard Wyroll (www.liqiditaetsplanung.de)
- Das Produkt *ValueNavigator* von RMCE RiskCon, Future Value Group und MIS (www.rmce.de)
- Das Produkt *GUARDEAN* von SHS Informationssysteme (www.shs.de)

Anhang 2: IT-Leistungen von IT-Outsourcingnehmern

(Quelle: http://www.it-vergabe.de/www.outsourcing-info.de/strategischeueberlegungen.pdf)



Anhang 3: Übersicht Leitfaden 1

Die nachfolgende Übersicht gibt einen Überblick über die Schritte, die im Leitfaden zur Schaffung der Rahmenbedingungen für ein erfolgreiches Risiko-Management gemacht werden sollten:

1	Klärung der Rahmenbedingungen des Risiko-Managements
2	Heranziehen des IT-Risiko-Managements
3	Benennung eines Risikoverantwortlichen
4	Etablierung des Risiko-Management-Prozesses in die Projektorganisation
5	Einbindung der Projektmitglieder
6	Kontinuierliche Information und Kommunikation aller Beteiligten
7	Weitergabe der Risikoinformationen an das unternehmensweite Risiko-Management

Anhang 4: Übersicht Leitfaden 2

Die nachfolgende Übersicht gibt einen Überblick über die Schritte, die im Leitfaden zum Risiko-Managment beim Outsourcing von IT gemacht werden sollten:

1 Anwendung des Risiko-Management-Prozesses für allen Phasen des IT-Outsourcings
2 Identifikation der Risiken bei einem IT-Outsourcing-Projekt
3 Vorgehensweise zur Risikoidentifikation
4 Nutzung von Hilfsmitteln für die Identifikation von Risiken
5 Nutzung von internen Quellen für die Identifikation von Risiken
6 Nutzung von externen Informationsquellen zur Identifikation von Risiken
7 Bewertung der Risiken bei einem IT-Outsourcing-Projekt
8 Beurteilung der Eintrittswahrscheinlichkeiten und der Auswirkungen von Risiken
9 Berücksichtigung der Wechselbeziehungen von Risiken
10 Unterscheidung von Primär- und Sekundärrisiken
11 Steuerung der Risiken bei einem IT-Outsourcing-Projekt
12 Einbindung der Entscheidungsträger
13 Festlegung von Risikostrategien
14 Nutzung der Möglichkeiten des IT-Outsourcings zur Risikosteuerung
15 Notwendigkeit einer besonderen Aufmerksamkeit bei der Partnerwahl
16 Steuerung durch den Outsourcing-Vertrag
17 Nutzung der Service Level Agreements
18 Erstellung eines IT-Sicherheitskonzepts zur Steuerung der IT-Risiken
19 Information und Kommunikation aller beteiligten Einheiten
20 Entwicklung von Notfallplänen
21 Überwachung der Risiken bei einem IT-Outsourcing-Projekt
22 Berücksichtigung des Restrisikos
23 Kontinuierliche Wiederholung des Risiko-Management-Prozesses
24 Vollständige Dokumentation des Risiko-Management-Prozesses

Literaturverzeichnis

Bea, F.X.; Göbel, E. (1999): Organisation. Lucius und Lucius-Verlag, Stuttgart 1999, S. 423-424.

Berg, J.; Gräber, H. (1995): Outsourcing in der Informationstechnologie: Eine strategische Management-Entscheidung. Campus, Frankfurt/Main, New York 1995.

Buchta, D.; Eul, M.; Schulte-Croonenberg, H. (2004): Strategisches IT-Management: Wert steigern, Leistung steuern, Kosten senken. 1. Aufl., Gabler, Wiesbaden 2004, S. 184-211.

Bullinger, H.-J.; Rüger, M.; Thiele, M. (1997): Erfolgsfaktoren des Outsourcing : Ergebnisse einer Studie; Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO, Stuttgart 1997, S. 19-29.

Bundesamt für Sicherheit in der Informationstechnik (2003): IT-Grundschutzhandbuch: Outsourcing. http://www.bsi.de/gshb/deutsch/menue.htm (Datum des Zugriffs: 20. Juli 2004).

Bundesamt für Sicherheit in der Informationstechnik (2003): IT-Grundschutzhandbuch: Mangelhafte IT-Sicherheit in der Outsourcing-Einführungsphase. http://www.bsi.de/gshb/deutsch/menue.htm (Datum des Zugriffs: 20. Juli 2004).

Bundesamt für Sicherheit in der Informationstechnik (2003): IT-Grundschutzhandbuch: Erstellung eines IT-Sicherheitskonzepts für das Outsourcing-Vorhaben. http://www.bsi.de/gshb/deutsch/menue.htm (Datum des Zugriffs: 20. Juli 2004).

Bundesamt für Sicherheit in der Informationstechnik (2003): IT-Grundschutzhandbuch: Schlechte oder fehlende Authentikation. http://www.bsi.de/gshb/deutsch/menue.htm (Datum des Zugriffs: 20. Juli 2004).

Bundesamt für Sicherheit in der Informationstechnik (2003): IT-Grundschutzhandbuch: Ausfall der Systeme eines Outsourcing-Dienstleisters. http://www.bsi.de/gshb/deutsch/menue.htm (Datum des Zugriffs: 20. Juli 2004).

Bundesamt für Sicherheit in der Informationstechnik (2003): IT-Grundschutzhandbuch: Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer. http://www.bsi.de/gshb/deutsch/menue.htm (Datum des Zugriffs: 20. Juli 2004).

Dörner, D., Horváth, P., Kagermann, H. (2000): Praxis des Risikomanagements : Grundlagen, Kategorien, branchenspezifische und strukturelle Aspekte. Schäffer-Poeschel, Stuttgart 2000, S. 380-413.

Dreger, W. (2000): Erfolgreiches Risiko-Management bei Projekten. Expert, Linde, Renningen 2000.

Edelbacher, M; Reither, P.; Preining, W. (2000): Sicherheits-Management: Grundlagen, Kosten/Nutzen im Unternehmen, technische Maßnahmen. Linde, Wien 2000. S. 257-258.

Gammelin, K. (2004): Raus damit! Damit beim Outsourcing nichts schief geht sind Controlling und RisikoManagement ein Muss. RiskNews, S. 25-30.

Gaulke, M. (2002): Risikomanagement in IT-Projekten. Oldenburg, München 2002, S.10-17.

Gaulke, M. (2000): Risk Map für IT-Risiken. http://risikomanagement-in-it-projekten.de/IT-Risiken/it-risiken.html (Datum des Zugriffs: 24. Mai 2004).

Gaulke, M. (2003): IT-Risikodimensionen. http://risikomanagement-in-it-projekten.de/IT-Risiken/IT-Risikodimensionen/it-risikodimensionen.html (Datum des Zugriffs: 24. Mai 2004).

Gaulke, M. (2004): Management von operativen Risiken. http://risikomanagement-in-it-projekten.de/Operative_Risiken/operative_risiken.html (Datum des Zugriffs: 24. Mai 2004).

Gernert, C.; Ahrend, N. (2002): IT-Management: System statt Chaos : ein praxisorientiertes Vorgehensmodell. 2., Aufl., Oldenburg, München 2002.

Gouge, I. (2003): Shaping the IT Organization – The Impact of Outsourcing and the New Business Model, Springer, London 2003 ,S.137-156.

Gumsheimer. T. (1994): Informationspartnerschaften: konzeptionelle Grundlagen für die Gestaltung von Partnerschaften im Informationsmanagement. Lang, Frankfurt/Main 1994.

Heilmann, H. (2003): IT-Projekt-Management - Fallstricke und Erfolgsfaktoren : Erfahrungsberichte aus der Praxis. 2. Aufl., dpunkt, Heidelberg 2003.

Hendrix, U.; Abendroth, C.; Wachtler, G. (2003): Outsourcing und Beschäftigung: die Folgen betriebsübergreifender Kooperation für die Gestaltung von Arbeit. 1. Aufl., Hampp, München, Mering 2003.

Hodel, M; Berger, A.; Risi, P. (2004): Outsourcing realisieren: Vorgehen für IT und Geschäftsprozesse zur nachhaltigen Steigerung des Unternehmenserfolges. 1. Aufl., Vieweg, Wiesbaden 2004.

Junginger, M. (1999): IT-Risk-Management – Identifikation, Analyse und Steuerung der Risiken des Informationsmanagements. Diplomarbeit, Universität Hohenheim, Stuttgart 1999

Kaeding, N. (2003): Rechtliche Gestaltung von Service Level Agreements. http://www.sla-info.de/artikel/gestaltung_SLA.pdf (Datum des Zugriffs: 30. Juli 2004).

Kendall, R. (1998): Risk Management : Unternehmensrisiken erkennen und bewältigen. Gabler, Wiesbaden 1998.

Kirchner, M. (2002): Risikomanagement : Problemaufriss und praktische Erfahrungen unter Einbeziehung eines sich ändernden unternehmerischen Umfeldes. Hampp, München, Mering, Hampp 2002, S.16-19; S. 37-51.

Köhler-Frost, W. (2002): Allianzen und Partnerschaften im IT-Outsourcing. KS-Energy, Berlin 2002, S. 83-149; S. 204.

Koppelmann, U. (1996): Outsourcing. Schäffer-Pöschel, Stuttgart 1996

KPMG (1998): Integriertes Risikomanagement. http://www.kpmg.de/services/ business_services/pdf/IRM.pdf (Datum des Zugriffs: 24. Mai 2004), S. 16-25.

Krallmann, H. (1989): EDV-Sicherheitsmanagement: Integrierte Sicherheitskonzepte für betriebliche Informations- und Kommunikationssysteme, Schmidt, Berlin 1997, S. 10-15.

Krcmar, H. (2003): Informationsmanagement. 3. Aufl., Springer, Berlin, Heidelberg, New York 2003, S.358-369.

Lichtenberg, G. (1992): Risiko-Management bei EDV-Projekten : technische und vertragliche Aspekte. Expert, Ehningen bei Böblingen 1992, S. 123-127.

Mangold, Pascal (2004): IT-Projekt-Management kompakt. 2. Aufl., Elsevier, München 2004.

MTR (2003): IT-Risikomanagement – Kostenfaktor, Notwendigkeit oder Chance für ihr Unternehmen. http://www.rosenheim.de/it_region/veranstaltungen/dokumente/ vortrag_risikomanagement_ohneShow.ppt (Datum des Zugriffs: 24. Mai 2004).

Müller, H.-E.; Prangenberg, A.(1997): Outsourcing-Management. Bund-Verlag, Köln 1997, S. 27-54.

Neubauer, M. (2003): Krisenmanagement in Projekten. 2. Aufl., Springer, Berlin, Heidelberg, New York 2003.

Pastors, P. M. (2002): Risiken des Unternehmens: vorbeugen und meistern. Hampp, München, Mering, Hampp 2002, S. 477-505.

Romeike, F.; Finke, R. B. (2003): Erfolgsfaktor Risiko-Management: Chance für Industrie und Handel ; Methoden, Beispiele, Checklisten. 1. Aufl., Gabler, Wiesbaden 2003, S. 147-183; S.235-247.

Schätzer, Silke (1999): Unternehmerische Outsourcing-Entscheidungen: eine transaktionskostentheoretische Analyse. Gabler, Wiesbaden 1999, S. 42-50.

Söbbing, T. (2002): Handbuch IT-Outsourcing: rechtliche, strategische und steuerliche Fragen. Mitp, Bonn 2002, s. 19-51.

Sparrow, E. (2003): Successful IT outsourcing : from choosing a provider to managing the project. Springer, London, Berlin, Heidelberg 2003, S. 195-209.

Stöger, R. (2004): Wirksames Projekt-Management. Schäffer-Poeschel, Stuttgart 2004.

TenStep (2000-2003): Risiko-Management / Techniken. http://www.tenstep.ch/7_2.php (Datum des Zugriffs: 24. Mai 2004).

TeraGate AG; Gabriel, T. L.(2002): IT-Outsourcing - Eine strategische Entscheidungshilfe. http://www.it-vergabe.de/www.outsourcing-info.de/strategischeueberlegungen.pdf (Datum des Zugriffs: 30.07.2004).

Versteegen, G. (2003): Risikomanagement in IT-Projekten : Gefahren rechtzeitig erkennen und meistern. Springer, Berlin, Heidelberg 2003.

Wallmüller, E. (2004): Risikomanagement für IT- und Software-Projekte: Ein Leitfaden für die Umsetzung in die Praxis. Hanser, München, Wien 2004.

Wißkirchen, F. (1999): Outsourcing-Projekte erfolgreich realisieren : Strategie, Konzept, Partnerauswahl; Schäffer-Poeschel, Stuttgart 1999, S.200-215.

Zahn, E.; Barth, T.; Hertweck, A. (1998): Leitfaden zum Outsourcing von unternehmensnahen Dienstleistungen. 1. Aufl., Industrie und Handelskammer Region Stuttgart, Stuttgart 1998.

4Managers (2004): Flexibilität durch strategische Fokussierung. http://www.4managers.de/01-Themen/..%5C10-Inhalte%5Casp%5Coutsourcing.asp?hm=1&um=O (Datum des Zugriffs: 30.7.2004).

Erklärung

Hiermit erkläre ich, dass ich die vorliegende Diplomarbeit selbständig angefertigt habe. Es wurden nur die in der Arbeit ausdrücklich benannten Quellen und Hilfsmittel benutzt. Wörtlich oder sinngemäß übernommenes Gedankengut habe ich als solches kenntlich gemacht.

Ort, Datum

Unterschrift