IT-Risiko- und Chancenmanagement im Unternehmen

Ein LEITFADEN für kleine und mittlere Unternehmen

BITKOM
Connecting visions - creating solutions

Impressum

Herausgeber:
BITKOM
Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.
Albrechtstraße 10
10117 Berlin-Mitte

Tel.: 030/27 576 – 0
Fax: 030/27 576 – 400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner:
Dr. Sandra Schulz
Tel: +49 (0)30 / 27576 – 242
E-Mail: s.schulz@bitkom.org

Die vorliegende Broschüre entstand in der BITKOM-Projektgruppe „IT-Risikomanagement in Unternehmen“ des Kompetenzbereiches Sicherheit.

Wir danken allen Mitgliedern und Gästen der Projektgruppe für das kontinuierliche Interesse am Thema, die wertvollen Diskussionen sowie die zahlreichen Anregungen. Besonderer Dank gilt den federführenden Autoren

- Armin Haase, Michael Schmidt (AXA Versicherung AG)
- Henry M. Hanau (secunet Security Networks AG)
- RA Bernd H. Harder (Harder Rechtsanwälte)
- Bernd Hausmann, Detlef Kilian (DS Data Systems GmbH)
- Helko Kögel (IABG Industrieanlagen- Betriebsgesellschaft mbH)
- RA Claus-Dieter Müller-Hengstenberg (Technische Universität München und Stuttgart)

Inhalt

Management Summary

Infolge der zunehmenden Globalisierung der Märkte und der immer kürzeren Entwicklungszyklen befinden sich die Unternehmen in einem Umfeld, welches durch einen stetigen Wandel wirtschaftlicher, technischer, politischer und kultureller Anforderungen, eine zunehmende wirtschaftliche, organisatorische betriebliche und technische Komplexität und einem daraus resultierenden steigenden Erfolgsdruck (Umsatz- und Profitsteigerungen) auszeichnet.

Die unterschiedlichen Erwartungen der Anteilseigner, Belegschaft, Öffentlichkeit, Behörden usw. an die Unternehmen, etwaige Unternehmensrisiken zu bewältigen und über jedes Risiko und die damit einhergehenden Gegenmaßnahmen zur Risikobewältigung zu berichten, erfordern die Etablierung eines gesamtunternehmerischen Risiko- und Chancenmanagements. Zusätzlich gibt es rechtliche, betriebliche und wirtschaftliche Gründe für die Etablierung eines Risikomanagements.

Betrachtet man die Entwicklung, dass fast alle Unternehmen Informations- und Kommunikationstechnologie für ihr tägliches Geschäft nutzen, so sollte ein Risikomanagement für die IuK-Technologie (IT-Risikomanagement (IT-RM)) etabliert werden. Damit stellt das IT-RM einen wichtigen Teilaspekt im unternehmensweiten Risikomanagement dar.

Die Einführung eines IT-Risikomanagements im Unternehmen ermöglicht es, Bedrohungen frühzeitig zu erkennen, aber auch positive Geschäftsentwicklungen also Chancen aufzudecken. Dabei versteht man unter Risiko jede negative und unter Chance jede positive Abweichung von der vorgegebenen Zielgröße, wie z.B. den Planwerten der Gewinn- und Verlustrechnung. Daher spricht man in diesem Zusammenhang auch von IT-Risiko- und Chancenmanagement (IT-RCM). Das IT-RCM muss in bestehende Prozesse z. B. der IT-Strategie, dem IT-Sicherheitsmanagement eingegliedert und angepasst werden. Das IT-RCM durchläuft folgenden Prozesskreislauf: Risikoidentifikation, -analyse und –bewertung, behandlung und –überwachung. Verantwortet wird dies von einem IT-Risikomanager. Die Ergebnisse des IT-RCM-Prozesses werden den Verantwortlichen im Unternehmen zur Verfügung gestellt, um entsprechende IT-Sicherheitsmaßnahmen zu ergreifen.

Geschäftsführern wird dies immer bewusster: Nach einer Umfrage[1] aus 2005 investieren Manager verstärkt in die Sicherheit ihrer ITK-Systeme aufgrund von gesetzlichen Vorgaben. Die Einhaltung der Gesetze im Bereich Informationssicherheit (Compliance) ist für sie wichtiger als der Schutz vor Viren und Würmer.

[1] Quelle: Ernst & Young (Global Information Security Survey 2005), Computerwoche 49/2005

1 Zielsetzung des Leitfadens

Der Leitfaden soll Führungskräften das Thema IT-Sicherheit und die daraus entstehende Notwendigkeit für das entsprechende IT-Risikomanagement näher bringen. Er soll auch den Blick auf das damit verbundene Chancenmanagement im eigenen Unternehmen öffnen. Der Leitfaden richtet sich in erster Linie an diejenigen Führungskräfte, die aufgrund ihrer Funktion für die gesamte Thematik zwar verantwortlich sind, sich aber nicht überwiegend in einem eigenen Kompetenzbereich damit beschäftigen.

Der Leitfaden macht die Notwendigkeit eines effektiven und effizienten IT-Risikomanagements deutlich. Er gibt darüber hinaus erste Hilfestellung, die erforderlichen Maßnahmen auszuwählen und umzusetzen. Diese sind vielfältig, je nach Branche und Unternehmen und derzeitigem Status, können die Maßnahmen durchaus aufwändig werden.

Der Leitfaden erhebt keinen Anspruch auf Vollständigkeit. Er kann aufgrund des umfangreichen Themenspektrums des IT-Risikomanagements nur einen Empfehlungscharakter haben.

2 Ausgangssituation

Der Markt der Informations- und Kommunikations-(IuK-)Technologien ist einer der Märkte, der in den letzten Jahrzehnten schnell und überproportional gewachsen ist. Firewall, Router, Hub, Server, GPS - allein die Vielzahl der Schlagworte, die im Umgang mit solchen Technologien benutzt werden, lässt erahnen, dass es sich um sich rasant verändernde technologische Entwicklungen handelt.

Dabei steht der Begriff der IuK-Technologie für alle technischen Mittel, die der Verarbeitung oder Übertragung von Informationen und Sprache dienen. Zur Verarbeitung von Informationen und Sprache gehören Erhebung, Erfassung, Nutzung, Speicherung, Übermittlung, Verarbeitung, Darstellung und Ausgabe von Informationen und Sprache.

Die Anwendung von IuK (nachfolgend nur IT genannt) in Unternehmen, ist im heutigen intra- und interorganisationellen Zeitalter nicht nur Standard, sondern stellt häufig sogar einen entscheidenden Erfolgsfaktor dar. Grundsätzlich wird der wesentliche Erfolg eines Unternehmens also primär durch die optimal gestalteten Beziehungen zu sämtlichen Märkten, in denen sich das Unternehmen bewegt, bestimmt. Zu diesen Märkten zählen insbesondere

- der Beschaffungsmarkt
- der Personalmarkt
- der Absatzmarkt und
- der Kapitalmarkt

Man denke nur an das Modell der Just-In-Time-Produktion und -Lieferung, die organisatorisch und logistisch essentiell von einer reibungslos funktionierenden IuK-Technologie abhängt. Bei Unternehmen, die der Supply-Chain der Automobilindustrie angehören wollen, ist es unverzichtbare Voraussetzung, IT zu implementieren, da man ansonsten als potenzieller Geschäftspartner nicht in die engere Auswahl kommt. Der Automobilhersteller besichtigt und bewertet im Rahmen eines Audits nämlich die Qualität der Produkte, aber auch die Zuverlässigkeit des Zulieferers in puncto Lieferpünktlichkeit und Kontinuität.

Zu beachten ist weiterhin, dass die Abhängigkeit von der IT – sowohl in betrieblicher als auch in wirtschaftlicher Hinsicht – stark mit der jeweiligen Unternehmensbranche und –größe zusammenhängt. Ein Handwerksunternehmen mit nur einigen wenigen Angestellten, wird auf den Ausfall der IT wesentlich unempfindlicher reagieren als z.B. ein Finanzdienstleister, dessen Wertschöpfungsaktivitäten sich größtenteils auf die Darstellung und Verarbeitung von Informationen konzentrieren.

Längst werden diese modernen Technologien von Unternehmen als Instrument in allen Unternehmensbereichen eingesetzt, weil deren Anwendung sich verbessernd auf Performance, Service

und Workflow auswirken, u. a. aufgrund des damit erreichten besseren Informationsflusses. Häufig hängen aber der gesamte Geschäftsablauf bzw. die Wertschöpfungsaktivitäten elementar von der IT ab. Die Tatsache, dass sich eine optimal funktionierende Technologie durch Prozesse sämtlicher Unternehmensbereiche zieht und im Idealfall für einen reibungslosen Geschäftsablauf sorgt, birgt natürlich andererseits die Risiken, dass bei ihrem Versagen u. U. sämtliche Wertschöpfungsaktivitäten gestört werden oder komplett ausfallen.

Hier kann ein IT-Risikomanagement (IT-RM) unterstützen. Dabei versteht man unter Risiko jede negative - und unter Chance jede positive Abweichung von den vorgegebenen Planwerten. Hierbei dient das IT-Risiko- und Chancenmanagement (IT-RCM) der Absicherung der vorgegebenen Planwerte. Das IT-Risiko- und Chancenmanagement muss aber in bestehende Unternehmensprozesse (siehe Kapitel 2.1) eingefügt sein:

- Unternehmensstrategie
- Risiko- und Chancenmanagement
- IT-Strategie
- IT-Sicherheitsmanagement

Die Einführung eines IT-RM wird aber auch durch juristische, betriebliche als auch wirtschaftliche Gründe (siehe Kapitel 2.2) getrieben.

2.1 Unternehmensprozesse und ihre Bedeutung für das IT-RCM

Die Abbildung 1 verdeutlicht die Abhängigkeiten zwischen Unternehmensstrategie, IT-Strategie, IT-Risikomanagement sowie IT Sicherheitsmanagement.

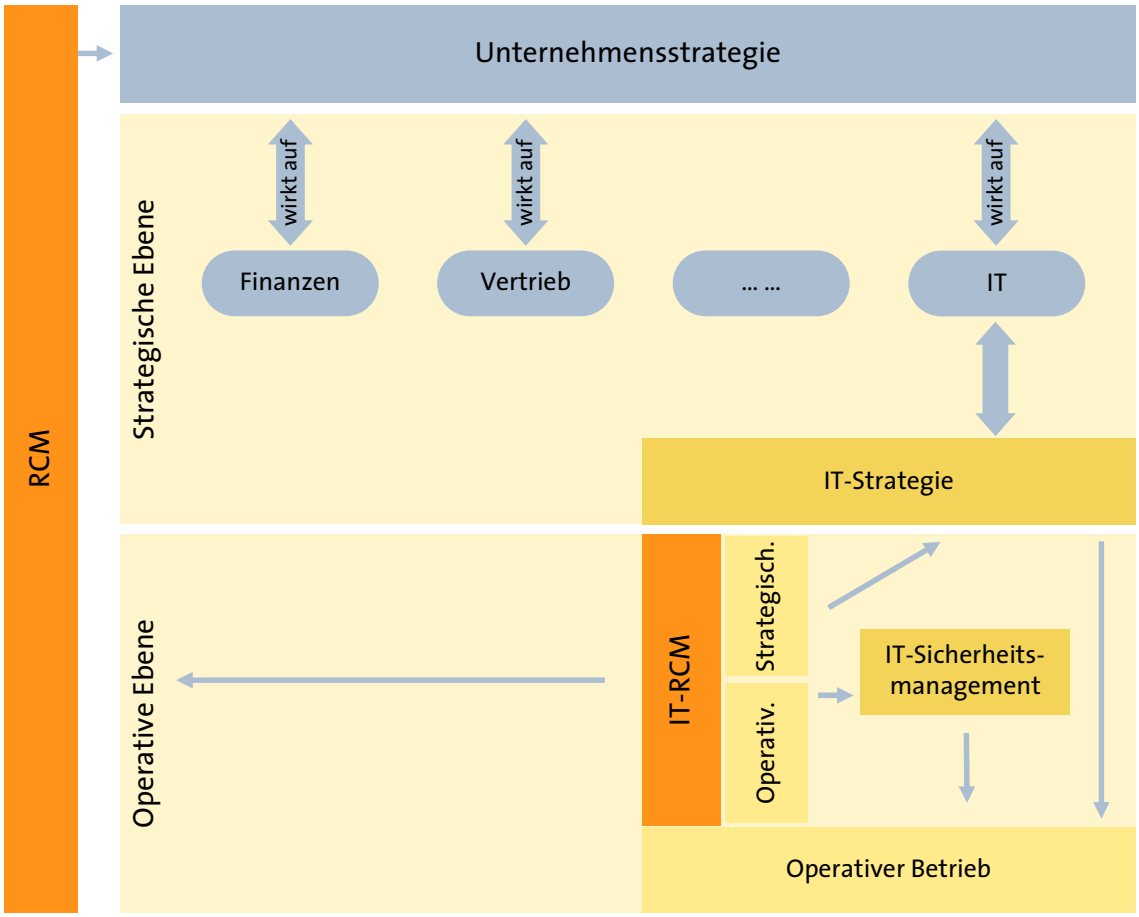

Abbildung 1: Schematische Darstellung der Beziehungen zwischen Unternehmensstrategie, IT-Strategie, IT-Risikomanagement und IT-Sicherheitsmanagement (Quelle: Hanau (selbsterstellt))

Im Folgenden werden die Prozesse und deren Auswirkung auf das IT-RCM erläutert.

2.1.1 Unternehmensstrategie

Der Begriff der Strategie bezeichnet im unternehmerischen Umfeld die höchste und abstrakteste Stufe der unternehmerischen Planung. Die Unternehmensstrategie teilt sich immer in zwei Handlungsmodule:

- Festlegung von angestrebten zukünftigen Zuständen des Unternehmens (Ziele, was will das Unternehmen erreichen); beispielsweise Kostenführerschaft im Marktsegment XY
- Festlegung der übergeordneten Handlungsleitlinien; beispielsweise Kostenführerschaft durch Senkung der Einkaufspreise um 20% in Planungszeitraum

Hieraus ergibt sich zwangsläufig eine mittel- bis langfristige zeitliche Orientierung sowie der zuvor benannte Abstraktionsgrad. Die Unternehmensstrategie ist die Leitlinie für alle lang- und mittelfristigen Planungen der einzelnen agierenden Einheiten des Unternehmens, also auch der IT.

2.1.2 Risiko- und Chancenmanagement

Die Aufgabe des Risiko- und Chancenmanagements (RCM) im Unternehmen besteht in erster Linie in der Existenzsicherung sowie der Absicherung der Unternehmensziele (Zukunftssicherung) unter leistungswirtschaftlichen, finanziellen und sozialen Aspekten, wobei die Risikokosten möglichst niedrig zu halten sind. Zur Erreichung dieser Ziele müssen wichtige Fragen beantwortet werden wie z. B.

- Welchen Risiken ist das Unternehmen jetzt und in Zukunft ausgesetzt?
- Welche Auswirkungen können die Risiken kurz- und langfristig haben?
- Wie ist mit den Risiken umzugehen?
- In welcher Weise können vorhandene oder entstehende Risiken vermieden, reduziert oder begrenztwerden?

Der Umgang mit Risiken erfordert einen klar strukturierten Managementprozess. Eine beispielhafte Auswahl von Unternehmensrisiken stellt die folgende Abbildung 2 dar:

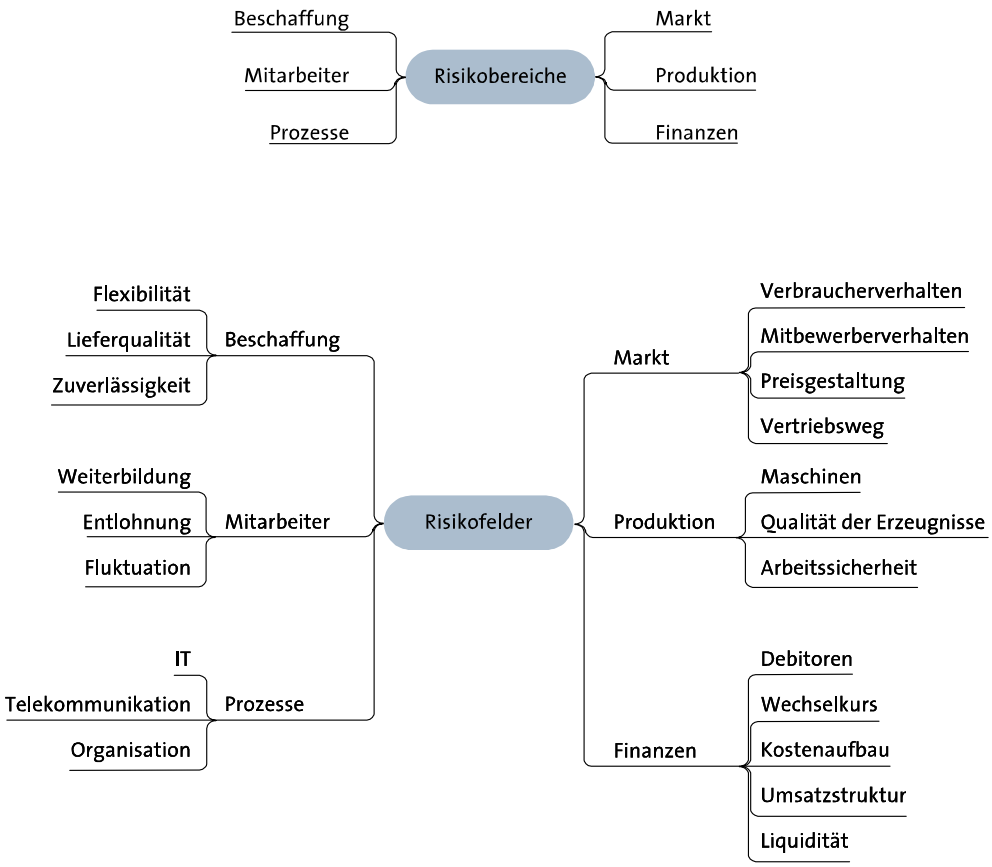

Abbildung 2: Schematische Darstellung ausgewählter unternehmerischer Risiken und der Felder Ihres Auftretens, Nach H. Jenny, Neuhausen, CH

Als RCM bezeichnet man die Summe all solcher Handlungen, die der frühzeitigen systematischen Erkennung, Bewertung und entsprechenden Behandlung von Chancen und Risiken dienen. Essentiell für jeden Teilaspekt von RCM ist zudem seine Dynamik, welche insbesondere für das gesamtunternehmerische RCM gilt. Viele Faktoren im unternehmerischen Umfeld, die Chancen und Risiken begründen, ändern sich mehr oder minder stark in mehr oder minder kurzen Zeitabständen (Bsp.: Unternehmenssteuern sind von eher zeitlich stabilen Charakter im Gegensatz zu sich schnell ändernden Kundenwünschen). Es ist das Wesen des Risiko- und Chancenmanagement sich damit auseinanderzusetzen. Dies ist jedoch nur als Prozess mit den sich im Zeitablauf wiederholenden Teilschritten „Erkennung, Bewertung, Behandlung und Überwachung“ möglich.

- Für die Berücksichtigung von Risiken und Chancen im Managementprozess ist die Bewertung ausschlaggebend, die sich vereinfacht in zwei Faktoren ausdrückt:
  - Die Höhe der Eintrittswahrscheinlichkeit (geschätzt, Plausibilität) und das Verhältnis von Risiko und Chance (nicht jedes Risiko und jede Chance ist würdig, gemanagt zu werden: z.B. „Firmenvernichtung durch Meteoriteneinschlag“ oder „Preisführerschaft durch die komplette Auslagerung aller Kernprozesse in Billiglohnländer“: beides denkbar, aber unrealistisch)
  - Der Grad der Beeinflussbarkeit der Chance und des Risikos durch das Unternehmen und der dazu notwendige Aufwand.
    Nur solche Risiken und Chancen, die aktiv beeinflussbar sind, kommen überhaupt in den Pool der managebaren Risiken und Chancen (R&C-Portfolios). Solche, die hiervon wiederum wirtschaftlich vertretbar beeinflussbar sind, werden selbst gemanagt.

Die klassischen Risikobegegnungsstrategien sind:

- Eingehen des Risikos
  (der rheinische Weg: ich tu nix, denn et han noch immer joot jejange)
- Vermeiden des Risikos
  (ich weiche aus, indem ich die risikobehaftete Handlung unterlasse. Allerdings vermeidet dies auch die Nutzung der evtl. verbundenen Chancen)
- Überwälzen des Risikos
  (ich finde jemanden, der mir die Last abnimmt: Versicherungen)
- Aktives Reduzieren des Risikos
  (ich werde selbst aktiv, um die Wahrscheinlichkeit des Scheiterns meiner Handlung zu verringern und diejenige des Gelingens zu erhöhen bzw. die Folgen abzumildern)

Gerne wird im täglichen Sprachgebrauch nur die letzte Risikobegegnungsstrategie mit dem gesamten Risikomanagement gleichgesetzt. Dies wäre allerdings zu kurz gegriffen, da man so die wichtigen Managementschritte „Erfassung“ und „Bewertung/Abwägung“ übergeht.

Das Feld der Chancenbegegnungstrategien hingegen ist recht überschaubar.

Bei abgewägten Chancen heißt es immer: realisieren!

Neben der rein sachlichen Beschäftigung mit Risiken und Chancen umfasst das betriebliche RCM auch eine organisatorische Komponente.

Im Rahmen des betrieblichen RCM gilt es, eine Infrastruktur in Form einer Aufbauorganisation, Zuordnung von Verantwortlichkeiten, Personal- und Mittelbereitstellung zu schaffen, die die zuvor benannte Erkennung, Bewertung und Behandlung von Chancen – und Risiken ermöglicht. Häufigste Organisationsform ist die Zuordnung zur Controlling-Abteilung bzw. eine Stabsstelle derselben.

Das allgemeine Risiko- und Chancenmanagement in Unternehmen ist seit langem in Deutschland gesetzlich reguliert (vgl. Abschnitt 2.2.1).

2.1.3 IT-Strategie

Die Unternehmensstrategie wird über Teilstrategien der einzelnen Bereiche sowie über operative Umsetzungspläne auf die einzelnen handelnden Einheiten heruntergebrochen.

Die IT-Strategie leitet sich somit aus der Unternehmensstrategie ab, da ihre Umsetzung den Wertbeitrag der IT zur Erfüllung der Gesamtunternehmensstrategie erbringen soll. Sie legt die zukünftigen Ziele der IT sowie die lang- und mittelfristigen Handlungsvorgaben zu ihrer Erreichung derselben innerhalb der Planungsperiode fest. Die IT-Strategie besitzt eine deutliche Schnittstelle zum Fokus dieses Leitfadens, dem IT-Risikomanagement. Da jede Strategie sich per definitionem mit der Erreichung zukünftiger Zustände (Ziele) beschäftigt, welche immer einer gewissen Unwägbarkeit des Gelingens und des Scheiterns unterliegt, ist die Zuführung der Ergebnisse des Managements strategischer IT-Risiken und Chancen sorgfältige Notwendigkeit einer jeden IT-Strategie.

2.1.4 IT-Sicherheitsmanagement

Ein weiterer Begriff im Zusammenhang mit IT-Risiken ist der des IT-Sicherheitsmanagements. Wie der Begriff schon andeutet, geht es um die Aufrechterhaltung des Schutzes von unternehmenseigenen Informationen und damit der Abwehr von Gefahren, die diese Informationen bedrohen. Unter IT-Sicherheitsmanagement versteht man alle zielgerichteten Handlungen, die der Wahrung der

- Vertraulichkeit (Geheimhaltung)
- Verfügbarkeit
- Verbindlichkeit
- Integrität

von IT-Systemen und den damit verarbeiteten Daten dienen.

Das IT-Sicherheitsmanagement ist im Vergleich zur IT-Strategie und dem IT-Risikomanagement stark operativ orientiert und stellt hierzu die folgenden Fragen in den Mittelpunkt:

- Wie sicher ist die IT ?
- Welche IT-Sicherheitsmaßnahmen müssen ergriffen werden ?
- Wie müssen diese Maßnahmen konkret umgesetzt werden ?
- Wie hält bzw. verbessert man das erreichte Sicherheitsniveau ?

Um die Aufrechterhaltung des Schutzniveaus im Zeitablauf zu gewährleisten, ist auch das IT-Sicherheitsmanagement als Prozess mit den sich wiederholenden Teilschritten

- Informationswertanalyse (Aufstellung der schützenswerten Informationen und Systeme)
- Schwachstellenanalyse
- Bedrohungsanalyse
- Risikoanalyse
- Planung der Abwehrmaßnahmen
  sowie
- Umsetzungskontrolle
  im Zeitablauf zu installieren.

Neben der rein sachlichen Beschäftigung mit Bedrohungen und Schutzmaßnahmen umfasst das IT-Sicherheitsmanagement auch eine organisatorische Komponente. Im Rahmen des IT-Sicherheitsmanagements gilt es, eine Infrastruktur in Form einer Aufbauorganisation, Zuordnung von Verantwortlichkeiten, Personal- und Mittelbereitstellung zu schaffen, die die Durchführung der zuvor benannten Teilschritte ermöglicht. Häufigste Organisationsform ist die Zuordnung als Stabsstelle zur IT-Abteilung.

Das IT-Sicherheitsmanagement ist der IT-Strategie untergeordnet und mit ihren Zielen in Einklang zu bringen. Des Weiteren setzt auch das IT-Sicherheitsmanagement die Ergebnisse des IT-RCM durch Behandlung der als managebar erkannten operativen IT-Risiken um.

2.2 Gründe für die Einführung von IT-RCM

In den folgenden Kapiteln sind rechtliche -, betriebliche und wirtschaftliche Gründe für die Einführung und den Betrieb eines IT-RCM dargelegt. Verständlicherweise kann eine klare Abgrenzung zwischen den drei Gründen nicht erfolgen. Zwischen ihnen gibt es Abhängigkeiten, so kann z. B. ein fehlerhafter Betriebsprozess wirtschaftliche Auswirkungen auf das Unternehmen haben.

2.2.1 Rechtliche Gründe

Grundsätzlich verpflichtet das Gesellschaftsrecht (§43 GmbH-Gesetz und §93 Aktiengesetz) die Verantwortungsträger in Deutschlands bedeutendsten Gesellschaftsformen zu einer sorgfältigen Geschäftsführung. Dies schließt natürlich die Pflicht zur Wahrnehmung von Chancen und zur Abwendung von gefährdenden Entwicklungen zum Nutzen der Gesellschaft implizit ein.

Die rechtliche Verpflichtung für die Einführung eines Risikomanagementsystems in Unternehmen ergibt sich insbesondere aus dem in das Aktienrecht eingeflossenen KonTraG, dem „Gesetz zur Kontrolle und Transparenz im Unternehmensbereich“ (§ 91, AktG). Damit sollen Kontrolle und Transparenz in Aktiengesellschaften und größeren GmbHs verbessert werden, z. B. indem ein Überwachungssystem eingeführt wird. Das Überwachungssystem soll frühzeitig Alarm schlagen, wenn die Existenz eines Unternehmens gefährdet ist. Dies betrifft nicht nur den Finanzbereich, sondern auch alle sonstigen Bereiche des Unternehmens, deren jeweilige Aktivitäten oder Handlungen zu finanziellen oder sonstigen materiellen Einbußen, Schäden oder sogar Unternehmenskrisen führen können. Mit dem Inkrafttreten des „Gesetzes zur Unternehmensintegrität und Modernisierung des Anfechtungsrechts (UMAG)“ im November 2005 wurde allerdings die Verantwortlichkeit eines Vorstands nach § 93 AktG sinnvoll relativiert. Dessen Absatz 1 Satz 2 lautet nunmehr: „Eine Pflichtverletzung liegt nicht vor, wenn das Vorstandsmitglied bei einer unternehmerischen Entscheidung vernünftigerweise annehmen durfte, auf der Grundlage angemessener Information zum Wohle der Gesellschaft zu handeln.“

Diese Regelung im Aktienrecht soll nach den Vorstellungen des Gesetzgebers (vgl. Gesetzesbegründung) auch für die größere GmbH Anwendung finden. Soweit Unternehmen Produkte herstellen oder vertreiben ergeben sich zusätzlich besondere unternehmerische Verantwortungen für die Einführung eines Risikomanagements. Dabei sind die in Sicherheitsnormen und technischen Richtlinien empfohlenen Maßnahmen ein (freiwilliger) Mindestmaßstab für die erforderlichen Verkehrssicherungspflichten der Produkte. Auch im Rahmen der vertraglichen Haftung für Pflichtverletzungen ist die Einhaltung von Sicherheitsnormen eine maßgebliche Frage für das Verschulden im Schadensfalle. Ein IT-Risikomanagement ist daher für ein Unternehmen notwendig.

Daneben gibt es staatlich initiierte, aber letztendlich freiwillige Bestrebungen der Wirtschaft, sich einen eigenen Verhaltenskodex unternehmerischen Handelns (neudeutsch: „Corporate Governance“) zu geben.

Auch international sind neue Regelwerke erlassen worden, die die Verantwortungsträger zu einer sorgfältigen und nachvollziehbaren Geschäftsführung verpflichten. Hier sei beispielhaft der Sabarnes-Oxley-Act im amerikanischen Rechtsraum genannt, der auch mittelbare Auswirkungen auf Unternehmen in Deutschland über US-Mutter- oder Tochtergesellschaften entfalten kann.

2.2.2 Wirtschaftliche Gründe

Der gezielte und effiziente Einsatz von IuK-Technologie hat zur Folge, dass geplante unternehmerische Ziele wie z.B. Kostensenkung und Gewinnsteigerung erreicht werden können. Voraussetzung dafür ist, dass sie verlässlich arbeitet und permanent zur Verfügung steht. In diesem Fall hat das Unternehmen die Chance, durch optimierte Bedingungen die geplanten wirtschaftlichen Ziele zu erreichen oder gar zu übertreffen.

Der unbestritten hohe Nutzen beim Einsatz von IT darf allerdings nicht darüber hinwegtäuschen, dass er auf der anderen Seite auch in vielerlei Hinsicht Risiken birgt, die sich schlimmstenfalls sogar existenzbedrohend auswirken können. Eine Betriebsunterbrechung, die sich auf den Ausfall der IT zurückführen lässt, kann auch eine Beeinträchtigung der Beziehungen zu Dritten nach sich ziehen. Dies gilt insbesondere, wenn Unternehmen Teil einer längeren Wertschöpfungskette sind:

- Funktioniert das Materialbeschaffungs-System nicht, kann es zu einem Engpass der benötigten Rohstoffe führen. Die Folge ist eine Unterbrechung des internen Betriebsablaufs mit erheblichen Umsatzeinbußen trotz der weiterhin anfallenden Fixkosten, z.B. für Personal und stillstehende Maschinen.
- Für einen Automobil-Zulieferer beispielsweise stellt das Materialbeschaffungs-System eines der Vielzahl von IT-Risiken dar, die für eine nicht fristgerechte Lieferung ursächlich sein können. Falls der Zulieferer seinen vertraglich vereinbarten Lieferverpflichtungen aufgrund einer Störung oder eines Ausfalls seiner IT nicht fristgerecht nachkommt, drohen ihm z.B. Pönalen, die üblicherweise mit dem Automobil-Hersteller in einem Service-Level-Agreement vereinbart werden.

Die wirtschaftlichen Vorteile eines IT-RCM lassen sich selten direkt mit einem monetären Nutzen messen. Vielmehr ist die belegbare Reduzierung und Begrenzung von Risiken ein Maß für die Vorteile, die ein ganzheitliches IT-RCM bietet. Gelingt es zudem, mit einer Vereinheitlichung und Standardisierung die Transparenz für das RCM für Dritte zu erhöhen, bringt dies weitere deutliche Vorteile mit sich:

a) Es trägt wesentlich zur Existenzsicherung bei, da Fehler oder gar Ausfälle der IT-Systeme erheblich reduziert werden.

b) Es kann in Verhandlungen mit potentiellen Kunden ein Kriterium sein, das deren Vertrauen in die Lieferfähigkeit erhöht und damit zur bevorzugten Auftragsvergabe gegenüber Wettbewerbern führt.

c) Gegenüber Banken kann das RCM vorgestellt werden, dessen Professionalität ein Baustein ist, der bei der Vergabe eines Rating-Urteils Berücksichtigung findet.

d) Schließlich stellen namhafte Versicherer als potentielle Risiko-Träger oftmals technische Mindestanforderungen an Schutzsysteme ohne die ein Risiko-Transfer in der Regel gar nicht vor-

genommen wird. Mittels gezielter Fragen wird der Stand des Risikomanagements aufgenommen und in die individuelle Prämienberechnung einbezogen. So werden bereits bisher für die Feuer- und Betriebsunterbrechnungs-Versicherung z.B. Brandfrüherkennungs-Systeme und automatische Feuerlöschanlagen berücksichtigt, die je nach Ausführung unterschiedlichen Schutzwerte erhalten, die zu günstigeren Versicherungsprämien führen können.

2.2.3 Betriebliche Gründe

Betrieblich lassen sich IT-Prozesse, wie die Informationsbeschaffung, -verarbeitung und -verteilung schneller, effizienter und vor allem transparenter realisieren. In diesem Zusammenhang gelingt es, auch eine Vielzahl von Prozessen zu automatisieren. Zudem ist IuK-Technologie extrem flexibel und dezentral einsetzbar. Die Flexibilität zeigt sich bei der Vernetzung von dezentralen Unternehmensstandorten. Die damit verbundenen informationsbasierten Koordinationstätigkeiten werden effizienter und produktiver gelöst, so dass mit einer langfristigen Kostenersparnis zu rechnen ist. Diese vielfältigen Einsatz- und Einsparmöglichkeiten beinhalten IT-Risiken, die gemanagt werden müssen, z. B.:

- Hat ein Unternehmen den Betrieb seiner Server outgesourct, so hat das Outsourcingunternehmen Zugriff auf die gespeicherten Daten. Im Rahmen eines IT-RCM muss hier über entsprechende Verträge der Zugriff genau festgelegt werden. Entsprechende Kontrollmaßnahmen sind einzuleiten.
- Eine zu hohe Temperatur im Serverraum kann zu einem Ausfall der Hardware führen. Um den Betrieb sicherzustellen, ist eine Risikoanalyse notwendig. Im Rahmen des IT-RCM müssen hier Maßnahmen definiert werden, die einen solchen Ausfall verhindern bzw. begrenzen und ein saubere Inbetriebnahme der Hardware garantieren.

Zur Einführung eines IT-RCM bietet es sich an, Standards zu nutzen, um ein strukturiertes und schon vielfach eingesetztes Verfahren anzuwenden. Die sich z. B. z. Zt. in aller Munde befindliche IT Infrastructure Library (ITIL) ist eine aus dem angelsächsischen Behördenumfeld stammende Sammlung von sog. „best practices“ (bewährte Vorgehensweisen), um die Erbringung von IT-Betriebsprozesse zu standardisieren, wirtschaftlich zu erbringen und ihre Qualität zu sichern. ITIL ist aber kein originärer Sicherheitsstandard. Derzeit existiert kein nationaler oder internationaler verbindlicher IT-RCM-Standard.

Da ein funktionierendes IT-Risikomanagement ein bewusstes IT-Sicherheitsmanagement einschließt, können IT-Sicherheitsmanagementstandards (z. B. ISO 27001, Bundesamt für Sicherheit in der Informationstechnik:BSI Standards 100), nach denen ein Unternehmen sich auch zertifizieren lassen kann, helfen. Ein Zertifikat stellt einen objektiven Nachweis über die Aktivitäten des Unternehmens im Bereich IT-RCM dar.

In dem BITKOM-Leitfaden „Kompass der IT-Sicherheitsstandards“ sind diese detailliert aufgeführt.

3 Einführung des IT-Risiko- und Chancenmanagements (IT-RCM)

Das IT-RCM setzt sich mit den IT-Risiken, der IT-Sicherheit und der Gewährleistung eines kontinuierlichen IT-Betriebes auseinander. Alle IT-Risiken, die die Liquidität oder den Unternehmenswert nachhaltig und deutlich beeinflussen oder gar die Existenz gefährden können, sind zu identifizieren, quantifizieren und dokumentieren (entsprechendes gilt für die sich ergebenden Chancen). Auch innerhalb des Bereiches des IT-RCM kann man zwischen strategischen und operativen Risiken und Chancen unterscheiden. Ein Beispiel für ein IT-RCM ist:

- Strategische Handlung: Umstellung der Softwarelandschaft auf OpenSource
  - Risiko: Scheitern bei der Aufrechterhaltung der bisherigen IT-Leistungen aufgrund von Inkompatibilitäten
  - Chance: Abkoppelung von langfristigen Lizenzabkommen und deren Kosten
- Operative Handlung: Umstellung auf OpenSource Webserver im Rahmen der OpenSource-Strategie
  - Risiko: Schlechtere Verfügbarkeit der Serverleistung aufgrund des noch mangelnden Know-Hows der Mitarbeiter
  - Chance: Erhöhte Flexibilisierung bei der Umsetzung von Änderungsanforderungen aufgrund des höheren Modularisierungsgrades der OpenSource-Software

Nur durch die Implementierung eines IT-RCM können alle wesentlichen Risiken erkannt und bewältigt werden.

Das IT-RCM sollte durch Personen im Unternehmen wahrgenommen werden (**IT-Risikomanager**), die sowohl IT und Technik - als auch kaufmännisches Verständnis und Erfahrungen haben. Er ist für die Steuerung des IT-RCM und in dieser Aufgabe dem Gesamtrisikomanagement verantwortlich. Besonders wichtig für ein IT-RCM ist die Übernahme von bewährten Methoden aus dem betriebswirtschaftlichen Bereich (Controlling), um eine nahtlose Übernahme und entsprechende Akzeptanz im allgemeinen betrieblichen Risikomanagement zu erreichen. Die rechtzeitige Weiterleitung aller dokumentierten IT-Risiken an die Geschäftsleitung erfolgt über das Controlling. Nur infolge eines zeitnahen Berichtswesens können sofortige Gegenmaßnahmen veranlasst werden.

Die Einführung eines IT-RCM kann nur dann von Erfolg gekrönt sein, wenn eine **Risikostrategie**, sie stellt die Grundlage des gesamten IT-Risikomanagement-Prozesses dar, entwickelt wird, die das Risikobewusstsein und die Risikokultur in die bestehende Unternehmenskultur impliziert. Nur durch den bewussten Umgang mit möglichen bzw. bestehenden IT-Risiken und den damit

verbundenen Chancen kann der Unternehmenswert gesteigert werden. Die Vorgabe der strategischen Ausrichtung ist in erster Linie die originäre Aufgabe der Geschäftsleitung.

Die Risikostrategie sollte folgende Grundsätze beinhalten:

- Etablierung eines Bewusstsein des jeweiligen Managements bzw. der Mitarbeiter in Bezug auf die Bedeutung und Rolle des IT-Risikomanagements für den Unternehmenserfolg
- Aufzeigen der Unternehmensstrategien und risikopolitischen Ziele des Unternehmens
- Implementierung von Standards hinsichtlich bestehender Regularien, Gesetze und Richtlinien
- eindeutige bzw. normierte Risikoklassifizierungen, -definitionen vornehmen, und somit eine Grundlage für die Risikoidentifikation zu schaffen
- Festlegung von Rollen und Verantwortlichkeiten (IT-Risikomanager)
- Festlegung der IT-Risikomethoden, -prozesse und Controllingmaßnahmen

Die Voraussetzungen für die Förderung des Risikobewusstseins sind Grundkenntnisse über das IT-RCM, die in Form von Workshops oder Schulungen vermittelt werden müssen. Neben dem Risikobewusstsein muss eine **Risikokultur** gelebt werden. Diese kann in Form von Workshops, Fachzeitschriften, internen IT-Policies bzw. entsprechenden Kompetenzen sichergestellt werden. Innerhalb eines Unternehmensverbundes sind alle Unternehmensbereiche, Funktionen und Prozesse mit einzubeziehen. Nur so können die entsprechenden Risiken sowie das Ausmaß etwaiger Schadensfälle durch die Prozess-Schnittstellen bzw. wechselseitigen Beziehung eruiert werden. Die eigene Risikokultur wird durch die Faktoren Personaleinsatz und –entwicklung, interne Kommunikation, fachliche Kompetenz der Mitarbeiter, Unternehmensphilosophie und Anpassungsfähigkeit hinsichtlich der sich ändernden Geschäftsprozesse geprägt.

Die **Risikopolitik** stellt einen Teil der Risikokultur dar, in welcher vorab definiert wird, welche Risiken bis zu welchen Schwellenwerten akzeptiert, vermindert bzw. gänzlich vermieden werden sollten. Im Fokus eines jeden Unternehmens steht die Maximierung der Chancen bzw. die Minimierung der Gefahren. Dem einzelnen Mitarbeiter des jeweiligen Unternehmens dient die Risikopolitik als Verhaltenskodex. Die grundsätzliche Vorgehensweise für den Umgang mit IT-Risiken wird durch die jeweiligen Unternehmensziele bestimmt. Damit eine Verbesserung des Risikobewusstseins ermöglicht wird, bedarf es einer einheitlichen Sprache/Definition bzw. Kommunikation.

Ein IT-RCM beinhaltet sowohl ein Frühwarn-, Überwachungs- als auch **Kontrollsystem**, um somit eine pro-aktive Überwachung etwaiger IT-Risiken zu gewährleisten. Mit Hilfe eines Frühwarnsystems können alle negativen Entwicklungen und die daraus resultierenden Risiken rechtzeitig erkannt werden. Das „Interne Kontrollsystem“ (IKS) bildet mit der internen bzw. externen Revision das so genannte Überwachungssystem und ist für die Sicherstellung zuverlässiger Geschäftsabläufe zuständig.

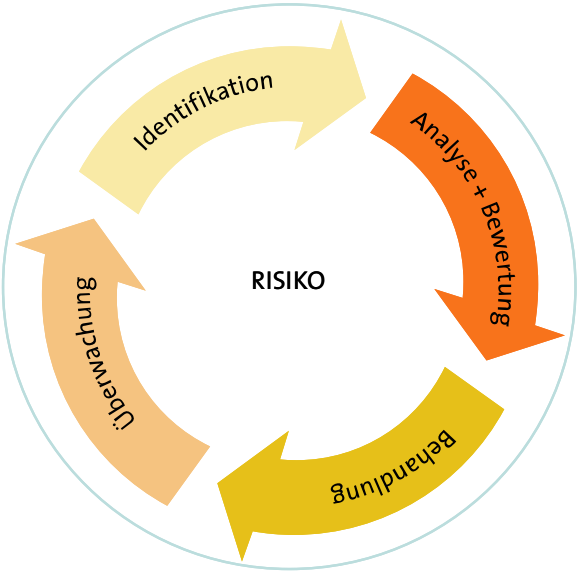

Abbildung 3: Prozesse des IT-RCM

Die Prozesse des IT-RCM bauen aufeinander auf und beeinflussen sich gegenseitig. Sie werden im Allgemeinen auch als Regelkreislauf dargestellt und setzen sich aus folgenden Elementen zusammen:

- Risikoidentifikation
- Risikoanalyse und –bewertung
- Risikobehandlung
- Risikoüberwachung

Die folgenden Kapitel sollen exemplarisch die einzelnen Schritte des o.g. Kreislaufmodells erläutern und Vorgehensweisen aufzeigen.

3.1 Risikoidentifikation

Die Risikoidentifikation beinhaltet eine strukturierte und kontinuierliche Ermittlung aller wesentlichen Risiken bzw. Risikobereiche.

Durch den stetigen Wandel der Umwelt und der Unternehmensprozesse entstehen immer wieder neuartige Risiken und bestehende Risiken verändern sich. Es müssen die auf die Unternehmensziele wirkenden Risiken erfasst werden, um somit den Auswirkungsgrad bzw. die Wechselwirkung eines Einzelrisikos auf die bestehenden Geschäftsprozesse feststellen zu können. Damit die Gesamtunternehmenssicht in dem Prozess Risikoidentifikation berücksichtigt wird, bedarf es eines Top-down-Vorgehens. Von der Unternehmensleitung ausgehend, müssen alle Unternehmensbereiche bzw. –prozesse mit integriert werden. In einzelnen Workshops identifizieren die Mitarbeiter und die Unternehmensleitung in Zusammenarbeit mit internen/externen IT-Sicherheitsspezialisten anhand einer bestehenden Risikosystematik, potentielle Risiken, die sich negativ auf die Unternehmensziele bzw. auf den Unternehmenserfolg auswirken können. Alle identifizierten Risiken bzw. Risikobereiche werden in einem Risikoinventar dokumentiert. Dieses Risikoinventar wird um die jeweiligen neu identifizierten Risiken ergänzt und dient als Grundlage für die darauf folgende Risikoanalyse.

Die ermittelten IT-Risiken können nach folgenden Bereichen kategorisiert werden:

- **Organisatorische Risiken**

Hierzu zählen beispielsweise die Outsourcing-Maßnahmen einzelner IT-Organisationen, die dazu führen, dass die Abhängigkeiten gegenüber dem Outsourcing-Nehmer zu Risiken (Abwanderung

von Fachpersonal, einseitiger Wissenstransfer, fehlende Kontrollinstanzen für die Qualitätsbewertung der Dienstleistungsqualität des externen Dienstleisters) führen können.

Ein weiterer Aspekt ist die nicht sachgemäße Aufgabenverteilung innerhalb der IT-Abteilungen, da die IT-Mitarbeiter nicht immer gemäß ihrer Qualifikation einzelnen Funktionsbereichen zugeordnet werden. So werden beispielsweise Anwendungsprogrammierer für die Systembetreuung und Mitarbeiter des Problem-Managements für die sofortige Fehlerbehebung eingesetzt, was zu Fehleinschätzungen, Verarbeitungsfehlern und Interessenkonflikten führt. Des Weiteren werden die IT-Abteilungen nicht ausreichend unabhängig in die jeweiligen Prozesse eingebunden. Sie sind vielmehr bestimmten strategischen IT-Entscheidungen unterworfen und können aufgrund dieser singulären Unternehmensinteressen nur eingeschränkt agieren.

Die in den Security-Policies dokumentierten IT-Sicherheitsmaßnahmen wie Passwortvergabe, Datensicherung etc. werden in den Unternehmen teilweise missachtet, so dass sensible Informationen bzw. Betriebsgeheimnisse für jedermann zugänglich sind. Das Risikobewusstsein der einzelnen Mitarbeiter muss aus diesem Grund ständig durch Workshop und Bekanntmachungen innerhalb des Unternehmens gefördert werden.

■ Rechtliche und wirtschaftliche Risiken

Alle Unternehmen halten eine Reihe von persönlichen Daten ihrer Mitarbeiter und auch Daten ihrer Kunden in Dateien vor. Die Abspeicherungen der persönlichen Daten der Mitarbeiter sind notwendige organisatorische Maßnahmen der Unternehmen. Die Vorhaltung von Kundendaten dient der Transparenz und Optimierung von Kundenbeziehungen. Soweit es sich hierbei jeweils um personenbezogene Daten handelt, unterliegen diese dem Schutz der Datenschutzgesetze und auch in gewissen Fällen dem Telekommunikationsgeheimnis (z.B. Telefon- oder Internetkommunikation).

Die Gefahr des Missbrauchs von geschützten Daten ist bekanntlich groß. Der Schutz dieser Daten bedarf einer Reihe von IT basierenden und konventionellen Schutzvorkehrungen wie zum Beispiel die Einrichtung von elektronischen Zugangskontrollen oder die Einrichtung von Passwörtern, Ablage von Datensammlungen in Panzerschränken usw.

Besonders schutzwürdig sind das Know-how, alle Betriebs- und Geschäftsgeheimnisse der Unternehmen (§ 17 UWG, § 20 UWG), die für den Wettbewerbsvorteil der Unternehmen maßgebend sind. Die Verletzung dieser Schutzgesetzes kann zu erheblichen finanziellen Schäden für ein Unternehmen führen. Daher sind in jedem Unternehmen erhebliche Schutzmaßnahmen erforderlich, die Verletzungen der Schutzgesetze unterbinden.

Die dem oben erwähnten Schutz dienenden Gesetze sehen viele Möglichkeiten vor, frühzeitig erkannte Verletzungsgefahren abzuwehren.

■ **Infrastrukturelle Risiken**

Nicht jedes Unternehmen weist standardisierte homogene IT-Infrastrukturen auf. Vielmehr existieren dort heterogene Hardwarekomponenten, Betriebssysteme (mit nicht immer aktuellen Release-Versionen) und Datenbanken. Durch die Inkompatibilitäten veralterter IT-Infrastrukturen kann es zu Kapazitätsengpässen führen, die einen Ausfall eines Teil- bzw. Komplettsystems zur Folge haben.

Weitere Risiken entstehen durch fehlende bautechnische Maßnahmen zur Absicherung des IT-Betriebs (Brandschutz), fehlende IT-Security-Prozesse bzw. Werkschutz (Verschlüsselung von geschäftskritischen Daten, Passwortvergabe, Zugangskontrollen, Überwachungssysteme etc.), wodurch der Schutz vor unberechtigtem Zutritt/Zugriff nicht gewährleistet werden kann.

Wenn Daten, Programme und betriebsnotwendige Dokumentationen nicht in regelmäßigen Abständen gesichert bzw. ausgelagert werden und keine Planungen und Vorkehrungen für den Notbetrieb und Wiederanlauf existieren, kann dies zu erheblichen Beeinträchtigungen des Betriebsablaufs und somit zu Vermögensverlusten führen.

■ **Applikations- und prozessbezogene Risiken**

Applikationsbezogene Risiken gehen von veralteten, eigenständigen Softwareversionen aus, die nicht in das Gesamtsystem integriert wurden und so genannte Insellösungen darstellen, z. B. der Jahr 2000-Umstellung. Aufgrund der fehlenden Schnittstellen zu anderen Applikationen werden teilweise manuelle Doppelerfassungen durchgeführt, die zu Eingabefehlern führen können und dadurch die Datenqualität stark beeinträchtigen.

Eine andere Problematik ergibt sich aus der unzureichenden Dokumentation von fremd- bzw. selbst erstellten Individualsoftwarelösungen, die eine nachträgliche Anpassung unmöglich machen, zumal das Entwicklungs-Know-how durch den jeweiligen Anwendungsprogrammierer teilweise nicht mehr zur Verfügung steht.

3.2 Risikoanalyse und -bewertung

Ausgehend vom erarbeiteten Risikoinventar erfolgt eine Risikoanalyse und –bewertung. Hier wird für die bedeutenden Risiken die Eintrittswahrscheinlichkeit und die mögliche Schadenshöhe ermittelt und festgelegt. Eine Risikoanalyse und -bewertung der Informations- und Kommunikationstechnik unterscheidet sich in Teilen von den Methoden der Versicherungsmathematik oder des Controllings. Die exakte Berechnung von Schadenshöhen und Eintrittswahrscheinlichkeiten bei einer quantitativen Risikoanalyse ist meistens nicht möglich, da geeignetes Zahlenmaterial fehlt.

Eine Methode zur Risikobewertung muss dennoch Bestandteil jedes Managementsystems für Informationssicherheit sein. Um ein Risiko bestimmen zu können, müssen die Bedrohungen

ermittelt und deren Schadenspotential und Eintrittswahrscheinlichkeit bewertet werden. Je nach Anwendungsfall, organisatorischen Randbedingungen, Branchenzugehörigkeit sowie angestrebtem IT-Sicherheitsniveau kommen unterschiedliche Methoden zur Risikobewertung in Frage. Das IT-Sicherheitsmanagement muss eine Methode auswählen, die für die Art und Größe der Institution angemessen ist. Die Methodenwahl beeinflusst entscheidend den Arbeitsaufwand für die Erstellung des IT-Sicherheitskonzepts. Ein Ansatz kann die IT-Grundschutz-Vorgehensweise des BSI sein. Kapitel 4.4 dieses Leitfadens stellt zudem eine Methodik vor, die dem IT-RCM einen Anschluß an das kaufmännisch dominierte Gesamtrisikomanagement der Unternehmung erlaubt und zudem in der Umsetzungsphase z.B. mit der Grundschutzmethodik kombiniert werden kann.

Die Qualifizierung der Risiken lässt sich nur dann einfach ermitteln, wenn bereits ein entsprechendes IT-Controlling in den jeweiligen Unternehmen etabliert wurde. Dies ist jedoch in vielen Unternehmen noch sehr schwach ausgeprägt, IT-Wirtschaftlichkeitsberechnungen und interne IT-Leistungsverrechnung bilden in den IT-Abteilungen die Ausnahme. Anschließend muss festgelegt werden, wie mit dem Risiko umzugehen ist.

- Risiken mit einem hohen geschätzten Schadenpotential fordern Maßnahmen, die eine Begrenzung (nicht unbedingt: Nullreduktion) der Schadenhöhe zur Folge haben
- Risiken mit hoher geschätzter Eintrittswahrscheinlichkeit fordern Maßnahmen, die die Häufigkeit des Eintretens eindämmen

Es existieren vier typische Risikobegegnungsstrategien, die zur Erreichung eines oder beider Grundsätze geeignet sind:

1. Risikovermeidung
   Die Strategie der Risikovermeidung zielt auf die gänzliche Unterbindung eines Schadens ab. Dies geschieht durch Verzicht auf die risikobehaftete Handlung. Allerdings beraubt man sich so auch der Realisierung der mit dem Risiko verbundenen Chance.
2. Risikominderung
   Die Strategie der Risikominderung zielt auf die Herabsetzung des möglichen eintretenden Schadens bzw. auf die Verringerung der Wahrscheinlichkeit des Eintritts oder auf beides gleichzeitig ab.
3. Risikotransfer (Überwälzung)
   Beim Risikotransfer übernimmt ein Dritter die Schadenauswirkungen bei Eintreten eines Risikos. Dies geschieht i.a. über Versicherungen oder über sonstige Vereinbarungen zwischen Risikoträger und Risikonehmer (z.B. ist es üblich, daß im Falle des Outsourcings das Risiko des IT-Betriebs vom Unternehmen auf den Outsourcing-Anbieter übergeht und im Outsourcingvertrag festgelegt wird, daß dieser bei Betriebsproblemen einsteht (meistens finanziell über Pönale)).
   Durch den Bezug einer extern angebotenen und i.a. kostenpflichtigen Leistung (Transfer)

entsteht insb. bei der Risikoüberwälzung die Notwendigkeit einer Kosten/Nutzen-Betrachtung.

4. Risikoakzeptanz
   Das Risiko wird ohne weitere Behandlung hingenommen. Auf den ersten Blick kommt diese Variante nur für Risiken mit niedrigen Schadenerwartungen oder sehr seltenem Eintreten (oder beidem) in Frage. Je nach Risikobereitschaft und zu erwartender Chance muß dies allerdings nicht zwingend sein.

Nach Auswahl einer passend erscheinenden Risikobegegnungsstrategie und der Umsetzung der daraus folgenden Maßnahmen ist das Risiko i.a. nicht auf Null reduziert. Für das verbleibende Restrisiko kann erneut eine Risikobegegnungsstrategie gewählt werden, bis das Risikovolumen auf ein für das Unternehmen tragbares Maß gesenkt wurde (Mehrfachanwendung). Der Begriff des „tragbaren Maßes“ ist unternehmensindividuell und hängt von der Risikobereitschaft der Verantwortlichen (i.a. der Geschäftsleitung) in den jeweiligen Feldern der betrieblichen Aktivität ab. Hier kommt der Festlegung einer Risikopolitik eine entscheidende Bedeutung zu, die diese grundsätzliche Einstellung gegenüber Risiken in des Unternehmens fixiert und dem (IT-) Risikomanager Spielräume bei der Auswahl der Risikobegegnungsstrategien gibt.

Das Eingehen des Risikos ist eine Strategie, die automatisch immer am Ende der Behandlung eines Risikos eintritt. Wie oben erwähnt, ist einem Risiko finanziell sinnvoll nur bis zu einem bestimmten Grad zu begegnen. Das Restrisiko wird immer hingenommen. Somit darf auch die eigene Risikovorsorge in Form finanzieller Mittel zur Abfederung von Schäden aus eingetretenen eingegangenen Risiken in einer sorgfältigen Begegnungsstrategie nicht aus den Augen verloren werden.

3.3 Risikobehandlung

Nach Festlegung der Risikobegegnungsstrategie muss diese in Maßnahmen umgesetzt werden. Die Maßnahmen sind zunächst in personelle -, organisatorische -, technische – und infrastrukturelle Maßnahmen zu gliedern.

Anschließend erfolgt eine Konsolidierung der Maßnahmen zu einem Gesamtzusammenhang (Plan) und die Überprüfung auf Konsistenz und Vollständigkeit. Dann findet eine Kosten/Nutzen-Abwägung der Maßnahmen mit einer Restrisikoanalyse statt. Diese werden dann in die Unternehmensplanung integriert. Der daraus resultierende Plan ist dann die Grundlage für die Umsetzung der Maßnahmen. Die Prioritäten, Kosten und Abhängigkeiten sind darlegt.

Bei der Umsetzung der festgelegten IT-Sicherheitsmaßnahmen muss eine Überwachung der Wirksamkeit der Maßnahmen erfolgen.

3.4 Risikoüberwachung

Das IT-RCM und die konkrete Realisierung muss regelmäßig überprüft und überarbeitet werden. Da die installierte IuK-Technik stetig neuen Anforderungen angepasst wird. Außerdem werden

neue Bedrohungen und Schwachstellen in bereits implementierten Produkten und Konfigurationen gefunden. Die Überarbeitung sollte mindestens jährlich (abhängig von ggf. den gesetzlichen sowie regulatorischen Anforderungen) und zusätzlich anlassbezogen erfolgen.

Um Änderungen in der IT-Infrastruktur berücksichtigen zu können, beginnt die Überprüfung und Überarbeitung zunächst bei der Sicherheitspolicy sowie der Überprüfung des Geltungsbereiches. Die einzelnen Schritte des IT-RCM-Prozesses werden erneut durchlaufen, wobei alle Ergänzungen und Anpassungen dokumentiert sowie Maßnahmen eingeleitet werden. Für die Realisierung gelten die Regelungen für die Abwicklung von Projekten, vom Anforderungsmanagement bis hin zur Abnahme und Dokumentation.

Die „Reviews“ und „Audits“ sind von unabhängigen Beratungsunternehmen oder von der internen Audit- bzw. Revisionsorganisation periodisch durchzuführen. Die Ergebnisse sind in Form eines Berichts der Geschäftsführung, den betroffenen Unternehmensbereichsleitern, der internen Revision sowie der Rechtsabteilung mitzuteilen.

4 Praxisbeispiele und Fallstudien

Im folgenden Kapitel sind unterschiedliche Praxisbeispiele und Fallstudien zum IT-RCM zusammengetragen. Die ersten beiden Praxisbeispiele beschreiben die Einführung eines IT-RM-Prozesse in Unternehmen und deren sicherheitsrelevanten Ergebnisse. Das dritte Beispiel geht konkret auf IT-Risiken bei IT-Projekten ein. Im Kapitel 4.4 wird detailliert dargelegt, wie IT-Risiken im Rahmen der Risikoanalyse und –bewertung finanziell bewertet werden. Hieraus können sich Ableitungen für eigene Unternehmen ergeben. Das letzte Beispiel zeigt anschaulich wie eine Risikoanalyse in Form eines Audits vereinfacht für KMU durchgeführt werden kann.

4.1 IT-RCM bei einem Zulieferunternehmen

Im folgenden wird das IT-RCM bei einem fiktiven Unternehmen mit betriebswirtschaftlich fundierten und realistischen Finanz-, Markt- und Strategiedaten beschrieben[2].

Das Unternehmen ist ein mittelständisches inhabergeführtes Unternehmen aus den 70er Jahren, welches bis zum Jahre 1990 ausschließlich PVC-Rohre für den Installationsbedarf hergestellt hat. Dieses Geschäftsfeld ist bis heute Hauptumsatzträger mit einem Anteil von 50%. Im Jahre 1991 entstand das Geschäftsfeld Zulieferteile insbesondere für die Automobilindustrie durch die Schaffung eines neuen Standortes und Anfang 1997 kam die Klapp- und Stapelboxsparte hinzu. Die Umsatzanteile dieser Geschäftsfelder liegen heute bei 40% bzw. 10%. Ziel dieser Diversifikation war es, die starke Abhängigkeit des Unternehmens von der Bauindustrie zu reduzieren.

Durch den Bau des neuen Werkes für die Automobilteileproduktion stieg der Umsatz seit 1990 um rund 100%. Aktuell beträgt er ca. 25,6 Mio. € bei einem Materialaufwand von 12,9 Mio. €, Personalaufwand in Höhe von 6,5 Mio. € und sonstigen betrieblichen Aufwendungen von 4,2 Mio. €. Das geplante Betriebsergebnis wird ca. 520.000 € betragen.

Mit der Unterstützung durch externe Unternehmensberater für Risikomanagement wurden die Risiken des Unternehmens identifiziert, analysiert und bewertet. Neben den Marktrisiken, wie z.B. die Preisschwankungen des Kunststoffgranulats für die PVC-Rohre und Klappboxen wurden die Bereiche Strategie, Finanzmarkt, Recht und Leistungserstellung untersucht. Hierbei wurde festgestellt, dass die IT-Risiken der Wertschöpfung in dem Geschäftsfeld der Automobilteileproduktion eine besondere Rolle spielen.

Weitere Risiken im Zusammenhang mit der IT sind:

[2] Erstellt von der RMCE RiskCon GmbH unter Mitwirkung der AXA Risk & Claims Services GmbH

- Es gibt nur einen Mitarbeiter als Ansprechpartner für EDV-Probleme. Im Krankheitsfall muss unnötig viel Zeit für die Lösung auftretender Probleme aufgewendet werden. Einem Produktionsausfall durch einen Unternehmenswechsel dieses Mitarbeiters ist durch die Bindungsfristen im Arbeitsvertrag vorgebeugt. Es wird im Kündigungsfall, was aus derzeitiger Sicht des Mitarbeiters als Unwahrscheinlich angesehen wird, mit Mehrkosten von 20.000,- €, durch externe Personalbeschaffung, gerechnet.
- Des Weiteren sind die vorhandenen PCs noch nicht alle miteinander vernetzt, was den Informationsaustausch langsam und arbeitsaufwendig macht. Als Folge davon sind Probleme beim Einkauf festzustellen, da die aktuellen Lagerbestände nicht rechtzeitig gemeldet werden können.
- Weiterhin wird die Flexibilität der Produktionsanlagen, d.h. die Möglichkeit der schnellen Umrüstung bzw. Produktionsanpassung, nur ungenügend ausgenützt, da die dazu notwendigen Daten aus der Vertriebsabteilung erst mit Verzögerung eintreffen. Die beiden Produktionswerke an unterschiedlichen Standorten werden durch je einen zentralen Fertigungsleitrechner gesteuert, der für die zentrale Produktionsdaten- und Sollwertspeicherung sowie die Betriebsdatenerfassung zuständig ist. Die einzelnen Maschinen sind CNC-geregelt.

Insgesamt kann festgehalten werden, dass viele „Risiken“, die aus der IT herrühren eigentlich Prozessschwächen sind, deren Optimierung die Effizienz des Unternehmens steigern kann.

Ein echtes Risiko liegt dagegen im Bereich Zulieferteile. Ein möglicher Schaden der hier entstehen kann, ist die Unmöglichkeit der termingerechten Lieferung an den Automobilhersteller. Auf Grund der Just-in-Sequence-Lieferung, bei der das für ein Fahrzeug individuell produzierte Bauteil nur Minuten vor dem Verbauen an das Band gelangt, führen Lieferverzögerungen zu einer direkten Wirkung beim Automobilhersteller. Diese Verzögerungen führen u.a. zu einer direkten finanziellen Wirkung durch Pönale, die vertraglich gegen den Zulieferer festgesetzt sind.

Um eine mögliche Schadenwirkung abzuschätzen, wurde in einem Workshop eine Expertenrunde befragt, sie sich aus Mitarbeitern des Vertriebs, der Produktion, der Qualitätssicherung, der IT sowie des Controllings zusammensetzte. Gemeinsam mit den Beratern wurden verschiedene Modell-Szenarien erarbeitet, welche möglichen finanziellen Auswirkungen verschiedene denkbare Ereignisse haben können.

Als Worst Case wurde beschrieben, dass die vorrätigen Bauteile nicht mehr an den Kfz-Hersteller geliefert werden können. Mögliche Gründe hierfür können, ein Brand im Lager, ein LKW-Unfall des Spediteurs oder der Ausfall der Lagersteuerung sein. In den beiden ersten Fällen handelt es sich um höhere Gewalt, bzw. ein Fremdverschulden, das seitens des Automobilbauers nicht belangt werden kann. Der Ausfall der Lagersteuerung jedoch obliegt dem Einfluss des Unternehmens.

Bei näherer Analyse wurde festgestellt, dass die chaotische Lagerhaltung in dem betroffenen Hochregallager von einer dezentralen Steuereinheit geregelt wird. Eine redundante Auslegung der Hardwarekomponenten ist nur teilweise erfolgt, ein Backup der Daten wird täglich durchgeführt. In der Expertenrunde wurde daraufhin diskutiert, welche Ereignisse und Ursachen es gibt, die zu einer Lieferstörung führen können. Die realistischsten Einschätzungen waren ein Stromausfall, der das gesamte System über einen längeren Zeitraum ausfallen lässt, sowie ein Kurzschluss von Elektronikkomponenten im Serverraum, der die Hardware nachhaltig schädigt. Die Diskussion des zweiten Ereignisses zeigte, dass einzelne Spezialkomponenten auf Grund der hohen Kosten nicht als Reserve vorgehalten werden und die Wiederbeschaffung bis zu einer Woche dauert. Dieser Worst Case wurde herangezogen, um eine detailliertere monetäre Bewertung vorzunehmen:

- Bei einem Brand im Serverraum wären die direkten Kosten für die Sachschäden an Elektronik und Gebäude durch die abgeschlossenen Feuerversicherung gedeckt gewesen, da aber eine Elektronik- sowie eine Betriebsunterbrechungsversicherung nicht besteht, müssen die Kosten für die Ersatzteile komplett selbst getragen werden. Die Wiederbeschaffung ist mit 25.000 € anzusetzen.
- Da auf das System und damit auf die Lagerware nicht mehr zugegriffen werden kann, werde zum einen 5 Mitarbeiter in das Lager entsendet, die manuell nach verschiedenen Bauteilen suchen. Hieraus entstehen Zusatzaufwendungen für Personal in Höhe von 2 Tagen je 5 Personen. Der Aufwand für die 10 Personentage ist mit 5.000 € zu kalkulieren.
- Gleichzeitig wird geprüft, welche Bauteile noch auf dem Transportweg und beim OEM sind. Die Komponenten, die als nächste verbaut werden müssten, werden in Sonderschichten nachproduziert, um den Bandstillstand zu vermeiden oder zumindest so kurz wie möglich zu halten. Für die Sonderschichten entsteht Personalaufwand von 17.000 € sowie zusätzlicher Materialaufwand und sonstige Kosten von 16.500 €.
- Bezüglich des Bandstillstandes wird davon ausgegangen, dass ca. 30 Fahrzeuge betroffen sein werden, was mit einer Strafzahlung von 10.000 € je Fahrzeug einherginge. Der Vertrieb geht allerdings davon aus, dass gemeinsam mit dem Kunden eine Lösung gesucht und gefunden wird und die tatsächliche Pönale bei ca. 50%, d.h. 150.000 € liegen wird. Welche Auswirkungen dies auf zukünftige Aufträge haben wird ist ungewiss, mit Umsatzeinbußen muss aber gerechnet werden.

Verschiedene Teilnehmer des Workshops gingen im Vorfeld davon aus, dass ein Bandstillstand beim Kunden so gut wie ausgeschlossen ist, mussten dann aber feststellen, dass ein solches Ereignis, nach Expertenmeinung durchaus alle 10-20 Jahre eintreten kann, was einer Wahrscheinlichkeit von 5% bis 10 % entspricht. Der Gesamtaufwand des Schadens läge bei vorsichtiger Schätzung bei ca. 210 T€, was mehr als 40% des geplanten Betriebsergebnisses ausmacht, ein durchaus bedenklicher Wert.

In einem Folgeprojekt, wurde die IT und das Controlling beauftragt, verschiedene Bewältigungsmaßnahmen zu erörtern und deren Kosten zu ermitteln. Der geschätzte Aufwand für Versiche-

rungen, redundante Bauteile, Überspannungsschutz, sowie einer Ausweichlösung an einem räumlich getrennten Standort, um auch das Brand- und Stromausfallszenario zu minimieren, beläuft sich auf einmalig 30.000 € sowie jährlichen Folgekosten von 5.000 €.

In der Entscheidungsvorlage für die Geschäftsführung konnte somit aufgezeigt werden, dass der ROI für das proaktive IT-RCM vergleichbar ist mit den nicht eingetretenen Aufwendungen in Höhe von 210 T€ bei einer Investition von 30 T€, wobei der tatsächliche Wertbeitrag der Maßnahmen ungemein höher liegen wird, da die Image- und Umsatzauswirkungen bei der monetären Bewertung unberücksichtigt blieben.

Dieses praktische Beispiel zeigt, dass die Beurteilung von IT-Risiken aufgrund ihrer Wechselwirkung mit anderen Unternehmensbereichen immer interdisziplinär erfolgen sollte, da die Tragweite einzelner Ereignisse nicht für jedermann transparent sind. Nur so kann der Gesamtrisikoumfang beurteilt werden, um abzuwägen, welche Maßnahmen ein sinnvolles Kosten-Nutzen-Verhältnis haben und dem Unternehmen einen tatsächlichen Wertbeitrag beisteuern.

4.2 IT-RCM bei einem Dienstleistungsunternehmen

Im folgenden wird das IT-RCM in einem mittelständisches Unternehmen mit einer Zentrale und verschiedenen Niederlassungen in Deutschland, in denen das operative Geschäft getätigt wird, dargestellt.

Das Unternehmen bietet seinen Kunden unterschiedliche Dienstleistungen an. Hierbei werden für die Kunden deren Wertschöpfungsprozesse zur Lagerung, Konfektionierung und Versand übernommen. Die gesamte hierfür notwendige Prozesssteuerung und Datenhaltung erfolgt dezentral in den Rechenzentren der Niederlassungen. Um finanziellen Nachteilen durch Risiken aus der IT zu begegnen, werden Hardware, Netze und Stromversorgung redundant ausgelegt, indem z.B. ein Notstromaggregat installiert, regelmäßig geprüft und gewartet wird.

Bedeutsame Risiken, die ihren Ursprung in der IT haben können, bzw. sich auf die Verfügbarkeit der IT auswirken, hat das Unternehmen unter Kontrolle. Mit regelmäßigen Reviews und Audits wird dieser Standard für alle Niederlassungen angestrebt und Maßnahmen zur Verbesserung, falls Defizite aus dem Bestand festzustellen sind, angestoßen.

Jedoch gibt es eine Schnittstelle, die alle Niederlassungen aufweisen. Die gesamten Buchhaltungssysteme sowie verschiedene Steuerungssoftware werden nur in der Zentrale vorgehalten, an die alle Niederlassungen angebunden sind. Dieses Rechenzentrum in der Zentrale wurde zu einer Zeit errichtet, als die Anforderungen an die IT, im Vergleich zum heutigen Stand, noch relativ gering waren. Durch das Wachstum und die Geschäftsausweitung, ist die Infrastruktur an die Grenzen ihrer Leistungsfähigkeit gelangt:

- Die Räumlichkeiten sind war in zwei Brandabschnitte unterteilt, was aber bei einem Löschangriff der Feuerwehr den Wasserschaden nicht verhindern kann.

- Ebenso fehlt die redundante Auslegung der Stromversorgung. Bei dem Erstellen des nicht unwahrscheinlichen Szenarios eines Großbrandes in der IT-Zentrale, konnte festgestellt werden, dass ein Back-Up der Daten, mit maximal 24 Stunden Datenverlust, jederzeit möglich ist, da die Bänder an einem dritten Ort aufbewahrt werden, der in so großer Entfernung zum Standort liegt, dass eine Beeinträchtigung ausgeschlossen werden kann.

Bis zu dieser Stelle der Analyse konnte festgestellt werden, dass sich ein echter monetärer Schaden für das Gesamtunternehmen noch in einem vertretbaren Rahmen befindet. Das Unternehmen als ganzes, ist nach wie vor handlungsfähig, die Kundenaufträge können von den dezentralen Standorten abgearbeitet werden. Dieses Worst-Case-Szenario führt zwar zu deutlichen finanziellen Einbußen, kann aber den Bestand des Unternehmens nicht gefährden.

Bei der Diskussion mit verschiedenen Verantwortlichen, denen das o.g. Problem bekannt war, stellte sich allerdings heraus:

- Dass in der Zentrale, neben den Controlling-Systemen der Niederlassungen, für einen großen Kunden auch das gesamte Rechnungswesen inkl. Inventur und der Erstellung von Jahresabschlüssen für den Wirtschaftsprüfer und Aktionär vorgenommen wird.
- Die Wiederbeschaffungszeit bestimmter Hardware beträgt ein bis zwei Monate, da diese nicht "von der Stange" verfügbar ist. D.h., dass nach einem Schaden zwar die Daten verfügbar sind, aber eine Verarbeitung für mehrere Wochen unmöglich wird.

Bei der Tragweite, die dies für den Kunden hat und der Öffentlichkeitswirksamkeit, die ein solches Ereignis mit sich bringt, kann davon ausgegangen werden, dass die unmittelbaren und langfristig mittelbaren Auswirkungen dazu führen, dass das Unternehmen insolvent wird. Kurzfristig wird die Liquidität stark beeinträchtigt, während langfristig das Vertrauen der Kunden in das Unternehmen so schwer geschädigt ist, dass diese abwandern werden. Tatsächlich war diese Komplexität der Geschäftsführung unbekannt bzw. wurde in ihrer Tragweite negiert. Die Verantwortlichen in den Niederlassungen gehen davon aus, dass die Zentrale nach wenigen Tagen wieder verfügbar ist und vertrauen auf die Kompetenz der Spezialisten vor Ort.

Erst durch die Signalwirkung, die durch einen Externen hervorgerufen wurde, erreichte die Aufmerksamkeit ein Niveau, das ein unmittelbares Handeln folgen lies. Die Notwendigen Maßnahmen zur Existenzsicherung wurden ergriffen. Einheitliche Regelungen und Empfehlungen in Standards zu IT-RCM, hätten diese Aufmerksamkeit evtl. schon frühzeitiger geweckt.

4.3 IT-RCM bei IT-Projekten

Mit Hilfe der IT werden heutzutage alle wichtigen Geschäftsprozesse der Unternehmen abgebildet. Innerhalb der einzelnen IT-Projekte nimmt die IT-Organisation einen sehr entscheidenden unternehmensstrategischen Part wahr, da die erfolgreiche Abwicklung von Projekten die Wettbewerbsfähigkeit des eigenen Unternehmens wahrt. Alle Unternehmen sind darauf angewiesen, eine erfolgreiche (zeitgerechte und kostenoptimierte) Realisierung der IT-Projektvorhaben zu

gewährleisten. Trotz der hehren Zielsetzungen scheitern viele IT-Projekte durch falsches Zeitmanagement, Budgetüberschreitungen bzw. fehlendes Change Management. Gerade die Nichteinhaltung von Projektterminen - und die damit verbundene Nichtverfügbarkeit neuer Anwendungen zu einem gewünschten Zeitpunkt - können zu gravierenden Nachteilen eines Unternehmens im Wettbewerb führen.

Nur durch ein wohldefiniertes bzw. etabliertes IT-RCM werden die Projektleiter in die Lage versetzt, etwaige Projektrisiken frühzeitig zu erkennen und entsprechende Maßnahmenkataloge zu erstellen.

Von daher sollte folgendes Phasenmodell Grundlage für das technologisches Konzept sein, das die notwendigen Entwicklungsschritte mit Meilensteinen versehen, festlegt. Die Grundstruktur der Phasenkonzepte ist im Prinzip immer gleich:

- Systemanalyse
- Systemdesign (IT Architektur)
- Systemumsetzung oder Realisierung
- Installation
- Wartung und Pflege

Die Vorgehensmodelle basieren auf der Basis der Phasenkonzepte. Danach erhält jede Phase eine bestimmte Menge von Aktivitäten, die sich von den Aktivitäten anderer Phasen abgrenzt, und die an Eintritts- und Fertigstellungskriterien geknüpft werden.

Ein wichtiges Kriterium der Phasen.- und Vorgehensmodelle ist, dass keine neue Phase begonnen wird, wenn die vorherige Phase nicht erfolgreich und vertragsgemäß abgeschlossen ist.

Die Frage eines effizienten Risikomanagements stellt sich nicht erst nach Abschluss eines Entwicklungsvertrages oder während der Durchführung eines Projektes bzw. nach der Einführung in den produktiven Einsatz. Vielmehr beginnt ein effektives Risikomanagement bereits in der Phase vor der Definition des Entwicklungszieles und vor dem Vertragsabschluss.

Die Erfahrungen mit IT Projekten haben über Jahre hinweg gezeigt, dass die Ursachen vieler Risiken in IT Projekten vielfach in einer mangelhaften Beschreibung der Projektziele vor Projektstart bzw. Vertragsabschluss liegen. Die Risiken tauchen aber in der Regel erst während der Durchführung der Projekte oder bei Änderungen der IT Applikationen auf und verursachen erheblichen Änderungs- bzw. Korrekturaufwand.

Für ein effektives Risikomanagementsystem, das sowohl die Entwicklung von Produkten als auch die Früherkennung von Störungen im Gesamtzusammenhang mit dem Unternehmensgeschehen umfasst, reicht es nicht aus, dass nur Prozess für die Früherkennung von Risiken ein geführt wird.

Vielmehr ist die Einführung eines Qualitätsmanagementsystems erforderlich, das alle Produkt bezogenen Abläufe bzw. Aktivitäten betrifft.

Ein effektives Risikomanagement bewegt sich demzufolge auf vier Ebenen

1. Einführung einer Qualitätsmanagement-Organisation
2. Einführung QM Verfahrens
3. Einführung eines Risikomanagement Verfahrens ab dem Zeitpunkt der Entwicklung der Entwicklungsidee sozusagen „life time“
4. Rechtliche Absicherung der Anforderungen und Einhaltung der vertraglichen vereinbarten Leistungen

Im Prinzip geht es bei allen Entwicklungsprojekten um folgende grundsätzliche Fragen und Anforderungen:

- Was ist die Strategische Planung (strategische Unternehmensziele)?
- Wird die strategische Planung durch die Informationstechnologie beeinflusst?
- Wie kann die Geschäftsplanung aus der strategischen Planung abgeleitet werden?
- Wie kann die Informationssystemarchitektur an die Geschäftsziele angepasst werden?
- Wie kann die Kundenzufriedenheit am besten sichergestellt werden?

Die Fragestellungen sollten während des gesamten Entwicklungszeitraums bis zu produktiven Einsatz sowie bei der Wartung oder Pflege der Systeme über einen Prozess ständig überprüft und gegebenenfalls angepasst werden.

In der Praxis werden daher pro Phasenabschnitt eines Phasenkonzeptes Prozesse zur Überprüfung der „Reife“ der Ergebnisse bzw. des Status der einzelnen Phasen eingesetzt, die den Erfolg und die Qualität der Leistung absichern. Daraus folgen folgende organisatorische Notwendigkeiten:

- Abbau einer Organisation für QA Managementaufgaben
- Einführung eines Angebots- und Freigabe Verfahrens anhand eines Phasenkonzepts
- Einführung eines Risikomanagement (Checklisten und Auswertungsverfahren)
- Eskalationsverfahren

Die Einführung von Organisationen und Verfahren zur Absicherung des Entwicklungserfolges erfordern nicht nur technischen, sondern auch ein vertragliche Maßnahme und Vorkehrungen.

Die Aufgabe des Vertrages ist es, die Leistungs- und Verantwortungsstruktur der Vertragspartner sowie die organisatorischen Anforderungen unmissverständlich und verbindlich für alle Vertragsparteien im Vertrag festzulegen.

Die Einzelphasen sind in der Abbildung 4. dargestellt.

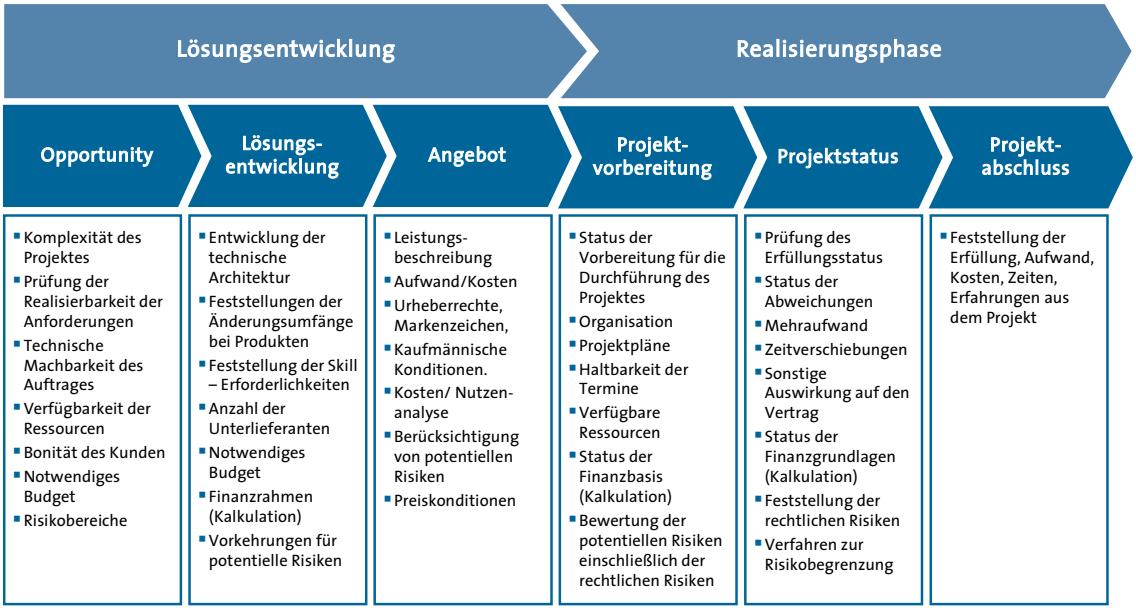

Abbildung 4: Einzelphasen der Lösungsentwicklung und Realisierungsphase

Die „Reviews“ und „Assessments“ sind von unabhängigen IT Experten periodisch durchzuführen. Die Ergebnisse sind in Form eines Berichts der Geschäftsführung, der Projektleitung und der Rechtsbeistand mitzuteilen. Die Geschäftsführung, die Projektleitungen, die Controlling/ Finanzabteilung und Rechtsbeistand sollten periodisch den Status der jeweiligen Phase abfragen und über Problemstellungen beraten bzw. entscheiden.

4.4 Methodik für IT-Risikoidentifikation und -bewertung

Im folgenden Beispiel wird in einem pragmatischen Ansatz gezeigt, wie IT-Risiken schnell finanziell bewertet werden können. Dies beinhaltet allerdings eine systembedingte Ungenauigkeit, die jedoch gewollt und im betrieblichen Alltag durchaus akzeptabel ist, da mathematisch genaue Verfahren höchst aufwendig sind und in keinem Verhältnis zum Nutzen im regulären Geschäftsbetrieb stehen.

Voraussetzung für das IT-RM ist es, Rollen mit Personen zu besetzen, die für die Ausführung der Schritte des Vorgehensmodells verantwortlich zeichnen. Kern aller Aktivitäten ist der IT-Risikomanager, der folgende Aufgaben hat:

- Schnittstelle zum allgemeinen betrieblichen Risikomanagement, um die Ergebnisse des eigenen IT-bezogenen Risikomanagements mit diesem kompatibel zu machen
- Schnittstelle zu den IT-Experten (wenn nicht selber mit entsprechender Expertise ausgestattet), um Informationen über Gefährdungen gegenüber IT-Systemen und deren Häufigkeiten zu erhalten (Integration der technischen Sicht)

- Schnittstelle zu den betrieblichen Fachbereichen, die IT zur Abwicklung ihrer Aufgabe nutzen, um Informationen über die Auswirkungen von Gefährdungen auf die benutzten IT-Systeme (Dienste) zu erhalten (Integration der betrieblichen Sicht)
- Einstufung, Filterung sowie Bewertung der erhobenen Risiken. Daraus folgend Ableitung von Risikobegegnungsstrategien und Erstellung von Entscheidungsvorlagen

Ziel ist es, IT-Risiken in monetären Größen auszudrücken, um den Finanzentscheidern des Unternehmens Anhaltspunkte für die zu treffende Vorsorge im IT-Bereich zu geben.

Jedem IT-Risikomanager sei deshalb geraten, Kontakt zur Instanz des allgemeinen betrieblichen Risikomanagements (i.a. Controlling-Abteilung) aufzunehmen und seine individuelle Ausführung der Aufgabe „IT-RCM“ an Begriffen und Kategorien dieser Instanz auszurichten bzw. zusammen zu entwickeln. Nur so ist ein Aufgehen des IT-RCM im Gesamtrisikomanagement mit entsprechender Akzeptanz möglich.

Ziel des Schrittes **Risikoidentifikation** ist die Abscheidung und eine erste grobe Bewertung der für das Unternehmen bedeutsamen und beeinflussbaren IT-Risiken aus der Gesamtmenge aller denkbaren Risiken, die auf die IT als Baustein des Unternehmens einwirken können. Hintergrund ist die nicht unbegrenzte Verfügbarkeit von Ressourcen zur Behandlung von Risiken, die eine Priorisierung und daran ausgerichtete Mittelverteilung erfordert.

Das folgende Trichtermodell (Abbildung 5) zeigt die einzelnen Schritte. Die vier Stufen werden im Folgenden näher erläutert.

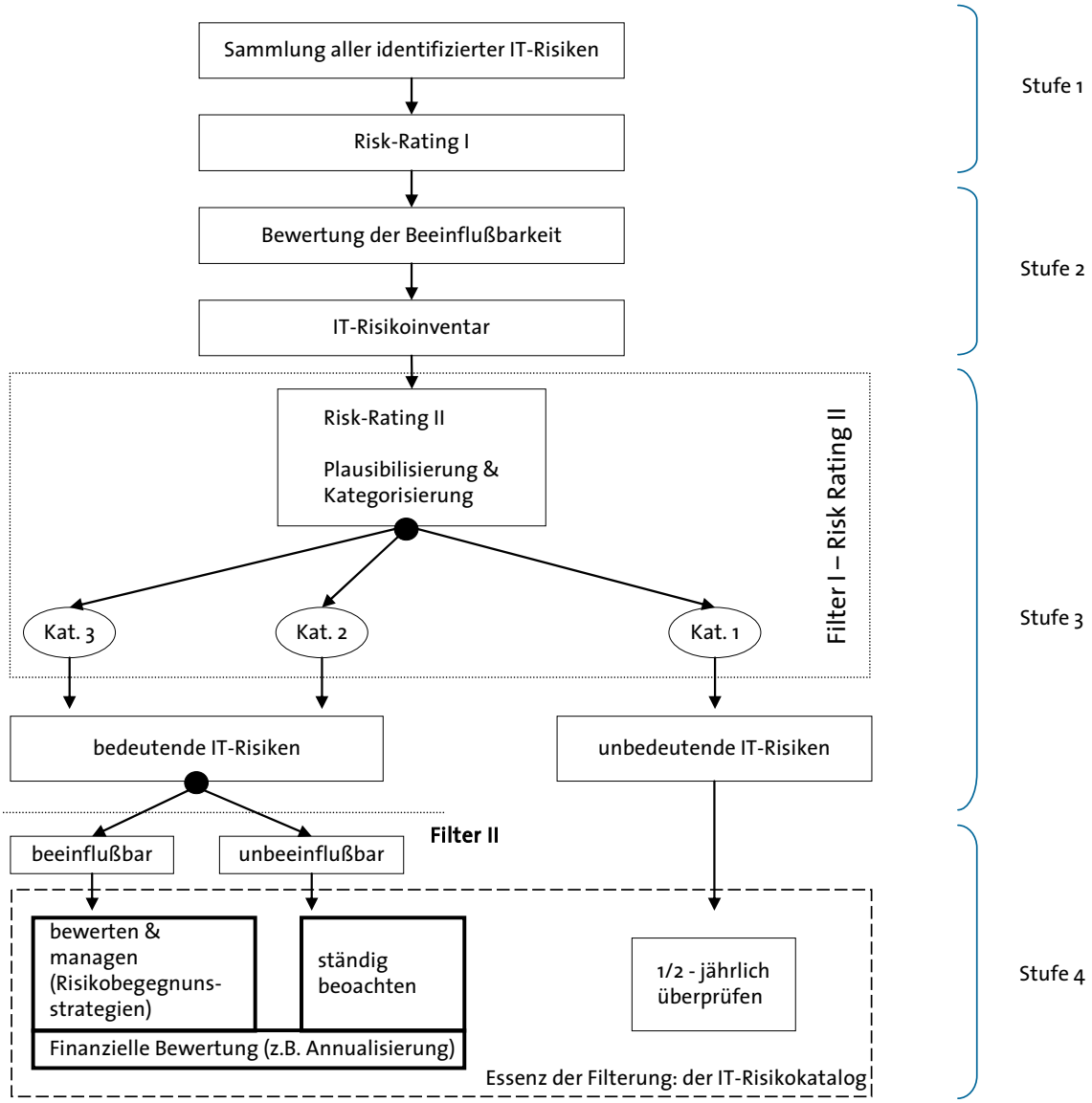

Abbildung 5: Trichtermodell zur Risikofilterung, selbsterstellt (Hanau) in Anlehnung an controller verein e.V.

■ Stufe 1) Risikoanalyse: Risk-Rating I

Ausgangspunkt aller Arbeiten ist eine erste vorgabenfreie Erhebung aller denkbaren IT-Risiken, die am besten in einem „Brainstorming“ mit den IT-Fachkräften durchgeführt werden sollte. Diese Liste ist i.a. sehr umfangreich und Bedarf einer ersten Filterung, zu welcher der IT-Risikomanager eine erste einfache Bewertung (Rating I) einsetzt, die wie folgt (siehe Abbildung 6) aussehen kann:

Rating	Risikobeschreibung
1	Unbedeutende Risiken, die kaum Auswirkungen auf die IT und das Unternehmen haben
2	Mittlere Risiken, die sich spürbar störend auf den IT-Betrieb und die darüber geführten Geschäftsprozesse auswirken und im Cash-Flow bzw Jahresergebnis des Unternehmens reduzierend spürbar sind.
3	Bedeutende Risiken, die deutliche Störungen des IT-Betrieb und der darüber geführten Geschäftsprozesse bewirken und Cash-Flow bzw Jahresergebnis des Unternehmens stark negativ beeinflussen.

Abbildung 6: Relevanzskala Risk-Rating I, selbsterstellt (Hanau) in Anlehnung an controller akademie

Die Zahl der Kategorien und ihr Inhalt sind durch den IT-Risikomanager frei wählbar und hier beispielhaft. Sie sollten jedoch mit dem Vorgehen des allgemeinen Risikomanagements im Unternehmen abgestimmt sein. Falls das allgemeine Risikomanagement die Kritikalität von Risiken mittels z.B. einer fünfstufigen Skala einordnet, sollte auch das IT-RCM mit fünf Stufen arbeiten oder eine Regel zum "umrechnen" aufgestellt werden.

■ Stufe 2) Risikoanalyse: IT-Riskinventar

Nach Erstellung der Risikoliste ist jedes erfasste IT-Risiko auf Beeinflussbarkeit (Managebarkeit) durch das Unternehmen zu prüfen. Dies führt zu einer deutlichen Segmentierung der initialen umfangreichen Risikoliste. Dies entstandene Liste in erster Ordnung bezeichnet man mit IT-Risikoinventar (siehe Abbildung 7).

Bereich / Ordnungsnummer (z.B. ITIL)	Risikoformulierung	Auswirkung/ Folgewirkung/ Wechselbeziehung	Maßnahmen zur Beherrschung (z.B. GSHB)	Risk-Rattingl	beeinfluss-bar (J/N)	
Portaldienst Configuration Management / PoCFM001	Mangelhaftes Patschmanagement	Manipulation/ Eindringen in das Portal Fehlbestellungen	Durchführung von Penetrationstests	2	J	1
Portaldienst Capacity Management / PoCPM001	unangepasste Vorhaltung von Rechenleistung/ Speicherplatz	verzögerte Reaktions-zeiten/ nachlassende Kundenloyalität/ Spitzen in Helpdeskanfragen	Kontinuierliche Auslastungsmessung/ Durchführen von Lasttests	3	J	2
Portaldienst Service Level Management / PoSLM001	rasche Änderung der Wünsche/ Anforderungen des Portalkunden	Änderung diverser Serviceprozesse/ erhöhte Kosten/ evtl. Abwanderung des Kunden	Einführung eines Key Account Managements zur Steuerung des Kunden/ Einführung einer gekapselten IT-Architektur	3	N	3

Abbildung 7: Ausschnitt aus einem IT-Risikoinventar, selbsterstellt (Hanau)

Für die grundsätzliche Struktur des Risikoinventars gibt es insb. auch im Bereich des Sicherheitsmanagements Check-Listen, die der IT-Risikomanager nutzen kann. Z.B. bietet das Grundschutzhandbuch des BSI für die Spalte 1 (Bereich/Ordnungsnummer) Vorgaben, anhand derer die Listung zu strukturieren wäre. Das o.g. Beispiel ist allerdings am Service-Portfolio des IT-Bereiches und den dahinterstehenden ITIL-Prozessen (vgl. Abschnitt 2.2.3) ausgerichtet, da mit der Verwendung dieser Systematik eine Berücksichtigung der über die IT geführten Geschäftsprozesse automatisch miterfolgt.

Die obige Tabelle führt als letzte Spalte in Geisterschrift die Zweitbewertung eines Stellvertreters des IT-Risikomanagers mit sich. Dieses Vorgehen dient der Verbesserung der Einschätzungsqualität, da mögliche Bewertungsdiskrepanzen zu einer erneuten Auseinandersetzung mit der Einschätzung führen (müssen). Es obliegt dem IT-Risikomanager und seiner Sicherheit im Umgang mit der Methodik, ob er diese Doppelbewertung durchführen läßt oder nicht.

- Stufe 3) Risikoanalyse: Risk-Rating II

Auf Basis des Risikoinventars wird nun die endgültige Trennung der Risiken in „wichtig“ und „unwichtig“ eingeleitet. Hierzu erfolgt eine Erweiterung der Bewertungsklassen; insbesondere kommt nun der Begriff des „Schadens“ in der Kategorisierung der Risiken in Verwendung. Zum sogenannten Risk-Rating II könnte z.B. die folgende Tabelle (siehe Abbildung 8) zur Relevanzeinordnung herangezogen werden:

Rating	Punktespektrum von	bis	Risikobeschreibung
1	3	4	Unbedeutende Risiken, die kaum Auswirkungen auf die IT und das Unternehmen haben
2	5	6	Mittlere Risiken, die sich spürbar störend auf den IT-Betrieb und die darüber geführten Geschäftsprozesse auswirken und im Cash-Flow bzw Jahresergebnis des Unternehmens reduzierend spürbar sind.
3	7	9	Bedeutende Risiken, die deutliche Störungen des IT-Betrieb und der darüber geführten Geschäftsprozesse bewirken und Cash-Flow bzw Jahresergebnis des Unternehmens stark negativ beeinflussen.

Abbildung 8: Relevanzskala Risk-Rating II, selbsterstellt (Hanau) in Anlehnung an controller akademie

Die Spreizung der Rating-Kategorien über ein Punktespektrum erfordert selbstverständlich eine Punkteermittlung für jedes Risiko, die exemplarisch wie folgt aussehen könnte:

Punkt-bewertung / Kategorie	Niedrig (1 Punkt)	Mittel (2 Punkte)	Hoch (3 Punkte)	Zeilenwert in Σ
Geschätzte finanzielle Auswirkung in Euro (Maßstab „1000“ Euro	kleiner 50	50-150	> 150	
Geschätzte Auswirkung auf die Außenwahrnehmung	keine/ leichte	mittlere	starke	
Geschätzte Eintrittswahrscheinlichkeit	gering	mittel	hoch	
Summer der Zeilenwerte				

Abbildung 9: Punkteskala zur Verwendung im Risk-Rating II, selbsterstellt (Hanau) in Anlehnung an controller akademie

Die Anzahl und Semantik der Kategorien (3 Stück, finanzielle Auswirkung, Image, geschätzte Eintrittswahrscheinlichkeit) sowie die Zahl der Punktbewertungen (3 Stück, niedrig, mittel, hoch) sind hier exemplarisch gewählt und müssen durch den IT-Risikomanager an die eigene betriebliche Wirklichkeit angepasst werden (es sind auch z. B. nur 2 Kategorien mit 5 Punktbewertung „vernachlässigbar“, „niedrig“, „spürbar“, „hoch“, „desaströs“ denkbar).

Auch hier sei darauf hingewiesen, daß die o. g. Kategorien und Punktebewertungen mit dem Vorgehen des allgemeinen Risikomanagements des Unternehmens abgestimmt sein müssen, so dass ein IT-Risiko der Kategorie 3 mit beispielhaften 8 Punkten auf identischem Bewertungsweg entstanden ist wie z. B. ein Marktrisiko oder Währungsrisiko derselben Kategorie aus dem betriebswirtschaftlichen Umfeld.

Hier liegt auch der deutliche Unterschied zu ähnlichen Bewertungsvorgehen bekannter IT-Sicherheitsstandards, die prinzipbedingt die Verbindung zum allgemeinen Risikomanagement des Unternehmens und die daraus als logische Konsequenz folgende sinnvolle Auseinandersetzung mit der Controlling-Abteilung nicht berücksichtigen (können).

Das Risk-Rating II ersetzt nun als Ordnungsattribut das Risk-Rating I und bildet zusammen mit dem bestehenden zweiten Kriterium der Beeinflußbarkeit des Risikos (dieses Kriterium wird durch das Risk-Rating II nicht beeinflußt) die finale Kategorisierung und Aufteilung der zur Disposition stehenden Risiken.

Das entstandene IT-Risikoinventar weist in der Kategorie „3 / beeinflußbar“ alle solchen IT-Risiken aus, die nun mit einer einzigen oder einem Mix der vier Risikobegegnungsstrategien angegangen werden müssen. Um die passende Strategie und daraus folgend die passenden Maßnahmen auswählen zu können, müssen die IT-Risiken dieser Kategorie zumindest einschätzungsmäßig finanziell bewertet werden.

- Stufe 4) Risikobewertung

IT-Risiken teilen mit einigen anderen Risikofelder des Unternehmens das Problem der Ermittlung der Schadenshöhe und Eintrittswahrscheinlichkeit und damit des Risikowertes, der auf dem Spiel steht. Auch hier existieren mathematisch exakte Verfahren (z. B. aus der Wahrscheinlichkeitsrechnung und der Spielsimulation), die aber aufgrund der nötigen Datenbasis und Softwaretools nur in den wenigsten Unternehmen vorhanden sein dürften. Aus diesem Grunde sei wie zuvor ein pragmatisches, wenn auch ungenaueres Verfahren vorgestellt, welches jedoch Ergebnisse von hinreichender Genauigkeit und vor allem finanzieller Aussagekraft produziert.

Für das sogenannte „Annualisierungsverfahren“ werden durch den IT-Risikomanager (evtl. mit entsprechender fachlicher externer Hilfe) realistische Zeitspannen definiert, in denen ein Schaden durch ein realisiertes Risiko eintreten wird. Gleichzeitig werden Schadenerwartungswerte eingeführt, die diesen Zeiträumen gegenüberstehen. Für jedes Einzelrisiko ist in der Folge anhand der gleichen Schadenzeiträume und Schadenerwartungswerte eine Bewertung und Verdichtung auf den Zeitraum „1 Jahr“ durchzuführen.

Sollte das allgemeine Risikomanagement des Unternehmens ebenfalls die Methode der Annualisierung zur Bewertung von Risiken heranziehen, ist es Aufgabe des IT-Risikomanagers, seine Definition der Zeiträume und Erwartungswerte mit denen des allgemeinen Risikomanagements zur Deckung zu bringen.

Zur besseren Verdeutlichung sei die Erwartungsaufteilung von Schadenshöhen gegenüber Zeiträumen für ein IT-Risiko beispielhaft anhand folgender Abbildung 10 verdeutlicht:

	Woche	Monat	Quartal	1 Jahr	3 Jahre
Realistischer Höchstsachden					600.000 €
Mitterer Schaden				100.000 €	
Kleinschaden		2.000 €			
Annualisierter Gesamtbewertungswert				**324.000 €**	

Abbildung 10: Annualisierungstabelle eines Einzelrisikos, selbsterstellt (Hanau) in Anlehnung an H. Jenny, CH.

Der annualisierte Gesamterwartungswert und damit die Höhe des Einzelrisikos berechnet sich aus 12*2000€ + 1*100.000€ + 0,3*600.000€ = 324.000 €

Diese Art der finanziellen Bewertung ist für alle Risiken der Kategorie „3 / beeinflußbar“ des IT-Risikoinventars durchzuführen. Über entsprechende Aggregationsmethoden ist zudem der Gesamtrisikoerwartungswert für den Bereich IT ermittelbar.

4.5 Vereinfachte Risikoanalyse im Form eines Audits

Häufig stellt sich gerade in KMUs die Frage, wie eine Risikoanalyse mit den zumeist begrenzt zur Verfügung stehenden Mitteln durchgeführt werden kann.

Der Erwartungswert von Risiken sind in der Praxis meist schwierig zu bestimmen, da die Eintrittswahrscheinlichkeiten aufgrund fehlender Basisdaten nur schwierig bestimmt werden können und die Ermittlung verlässlicher Daten sehr aufwändig ist.

Als pragmatisches Vorgehen in KMUs bietet sich hier eine vereinfachte Risikoanalyse in Form eines Audits an.

Folgende Vorgehensweise hat sich dabei als praktikabel erwiesen:

1. Kick-Off Veranstaltung
2. Risikoidentifikation: Durchführung eines Audits mit Vor-Ort Begehung
3. Risikoanalyse und –bewertung: Auswertung der Daten und Risikobewertung
4. Präsentation vor der Leitungsebene
5. Risikobehandlung

1. Kick-Off Veranstaltung

Die zwei- bis dreistündige Kick-Off Veranstaltung dient dazu, alle Beteiligten vorab über die anstehende Analyse zu informieren. Dazu zählen neben der Leitungsebene des Unternehmens alle Bereiche, in denen die Informationstechnik zur Unterstützung der Kerngeschäftsprozesse eingesetzt wird. Hinzugezogen werden sollten insbesondere auch Vertreter des Betriebs- bzw. des Personalrates. Gerade hier ist es sinnvoll, den Betriebsrat bereits vor der Untersuchung mit einzubeziehen, da eine Umsetzung von evtl. später erforderlichen organisatorischen Änderungen häufig wesentlich einfacher ist, als wenn der Betriebsrat erst in einer sehr späten Phase hinzugezogen wird.

Ziel der Kick-Off Veranstaltung ist somit die Vorstellung der verfolgten Ziele, Zeitpläne und Festlegung der einzelnen Interviewtermine. Dabei liegt es jeweils in dem Geschick des Auditors, die Mitarbeiter von der Notwendigkeit dieser Maßnahme zu überzeugen und nicht zu verängstigen.

Eine fehlende Aufklärung oder gar eine Verängstigung der Mitarbeiter führt später häufig dazu, dass dem Auditor entweder wichtige Informationen vorenthalten werden oder aber, dass er bewusst Fehlinformationen von den Mitarbeitern erhält. Auch kann eine solche Kick-Off Veranstaltung dazu verwendet werden, eine Sensibilisierung bzgl. der Bedeutung von Informationssicherheit für den Erhalt des Unternehmens durchzuführen. Der Umfang des Kick-Offs beträgt in diesem Fall 0,5 – 1 Tag.

2. Risikoidentifikation: Durchführung eines Audits mit Vor-Ort Begehung

In dieser Phase erfolgt die eigentliche Ist-Aufnahme. Der Auditor führt je nach Zielsetzung ein oder mehrere Interviews gemäß dem vorgestellten Zeitplan mit den definierten Ansprechpartnern durch und verifiziert die gemachten Angaben, indem er sich einen eigenen Eindruck vor Ort verschafft, die vorhandenen Dokumentationen überprüft und Angaben hinterfragt.

Als Grundlage bietet sich hier die Verwendung von Standards als Rahmenwerk an, beispielsweise die Verwendung der ISO 17799:2005 "Teil 1: Leitfaden zum Management von Informationssicherheit" und Teil 2: "Spezifikation für Informationssicherheits-Managementsysteme" (zukünftig ISO 27002) in Kombination mit Detailfragen aus dem deutschen Grundschutzhandbuch. Sofern das Unternehmen bereits über eigene Richtlinien verfügt, sollten diese mit in den Fragenkatalog aufgenommen werden. Die Verwendung von Standards zur Informationssicherheit bietet den großen Vorteil, dass diese mit ihren so genannten „Controls“ aus verschiedenen Managementbereichen den gesamten Geschäftsprozess einer Institution umschließen. Dieses bedeutet, dass nicht nur die technische IT-Sicherheit berücksichtigt wird, sondern vor allem Aspekte bzgl. des Managements der Informationssicherheit berücksichtigt werden. Hierzu gehören insbesondere die organisatorische Sicherheit und Aspekte, die sich aus gesetzlichen Vorgaben und Verträgen mit Geschäftspartnern ergeben.

3. Risikoanalyse und –bewertung: Auswertung der Daten und Risikobewertung

Nach Durchführung des Audits geht es nun darum, die vorhandenen Daten zu analysieren und zu bewerten. Hierbei ist es besonders wichtig, dass der Auditor unvoreingenommen ist und über eine große Erfahrung verfügt. Empfehlenswert ist es daher, das Audit von einem externen Dienstleister durchführen zu lassen, da hierbei auf einen großen Erfahrungsschatz zurückgegriffen werden kann und eine Unvoreingenommenheit besteht. Weiterhin wird einem externen Auditor meist ein Vertrauensvorschuss von den Mitarbeitern gegeben, oftmals erhält dieser Informationen, die ein interner Mitarbeiter nicht erhalten würde.

Bei der Auswertung erfolgt nun ein Abgleich der im Interview gemachten Angaben mit dem vor Ort gewonnenen Eindruck und einer Überprüfung von vorhandenen Unterlagen und Firmenrichtlinien. Der Umsetzungsgrad gemäß dem verwendeten Sicherheitsstandard wird für einzelne Bereiche ermittelt, wobei die für das Unternehmen nicht relevanten „Controls“ ausgeklammert werden. Anhand des zuvor ermittelten Schutzbedarfes für die Kerngeschäftsprozesse werden nun

die identifizierten Risiken erfasst und durch den Auditor bewertet. Die Risiken werden vereinfacht in drei Klassen („gering“, „mittel“ und „hoch“) eingestuft. Neben einer solchen Risikoabschätzung erfolgen meist noch Vorschläge[3] zum Ergreifen von Gegenmaßnahmen, bewertet nach der jeweiligen Dringlichkeit. Empfehlenswert sind hier auch die Benennung von Verantwortlichkeiten und eine Aufwandsabschätzung, soweit diese bereits gegeben werden kann.

4. Präsentation vor der Leitungsebene

Die Ergebnisse dieser Analyse werden nun der Leitungsebene vorgestellt (siehe Abbildung 11), die Entscheidungen werden begründet und diskutiert. An dieser Sitzung sollte dann zunächst auch nur die Leitungsebene teilnehmen, da die Ergebnisse der Risikoanalyse sensibel sind. Innerhalb dieser Veranstaltung sollte festgelegt werden, welche Informationen an die übrigen Beteiligten weitergegeben werden, da ein entsprechender Informationsbedarf besteht. Dieses ist notwendig, um die Mitarbeitersensibilisierung und die Bereitschaft zu Veränderungen zu erhöhen. Nur bei besonders sensiblen Risiken sollten diese lediglich einem kleinen Kreis der Leitungsebene zur Verfügung gestellt werden, um die Gefahr eines Missbrauchs zu verringern.

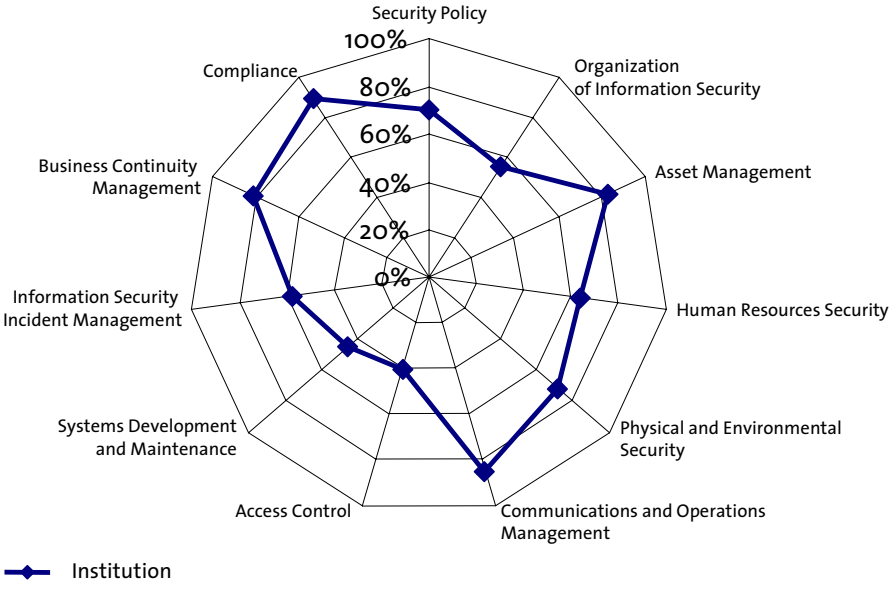

Abbildung 11: Für ein Management Summary bietet sich die Darstellung als Spinnennetz an.

[3] Anmerkung: Im Falle einer Zertifizierung auf Basis eines Sicherheitsstandards ist darauf zu achten, das Audit und Beratung voneinander getrennt sind. Im Falle einer dieser vereinfachten Sicherheitsanalyse ist das beschriebene Vorgehen legitim. Wird dennoch eine Zertifizierung angestrebt, muss für das Zertifizierungsaudit ein zweiter Auditor hinzugezogen werden.

5. Risikosteuerung

Nachdem die Ergebnisse der Untersuchung der Leitungsebene vorgestellt wurden, muss eine (schriftliche) Stellungnahme der Leitungsebene für den Umgang mit den Risiken erstellt werden. Dabei gilt es, für jedes identifizierte Risiko eine der folgenden Strategien zu wählen, wie diese bereits beschrieben wurden: Risikovermeidung, -minderung, -transfer bzw. –akzeptanz.

Wichtig dabei ist es, dass Zeitpläne und Zuständigkeiten bei nicht-akzeptablen Risiken bestimmt werden und entsprechende Budgets durch die Leitungsebene zur Verfügung gestellt werden.

Eine häufige Erkenntnis nach einem solchen Audit ist, dass bereits vielen Risiken durch Umstellung der Prozessorganisation wirksam begegnet werden kann, ohne dass große Budgets zur Verfügung gestellt werden oder aufwändige und komplizierte technische Systeme zum Einsatz kommen müssen. Meist kann hier bereits mit einfachen organisatorischen Maßnahmen sehr viel erreicht werden.

Der Vorteil der oben beschriebenen Methodik liegt darin, dass eine solche Vorgehensweise sehr schnell zu Ergebnissen führt und gerade deshalb für den Mittelstand geeignet ist. Schon mit einem externen Aufwand von 10-15 Tagen liegen grundlegende Ergebnisse vor, die die Basis für die weitere Risikosteuerung bilden.

5 Beitrag unserer Branche

Der BITKOM vertritt mehr als 1.000 Unternehmen aus der Informationswirtschaft, Telekommunikation und neue Medien. Zu den Mitgliedern zählen Geräte-Hersteller, Anbieter von Software, IT-Services, Beratungsleistungen, Telekommunikationsdiensten und Content. In den folgenden Kapiteln ist beispielhaft erläutert, welchen Beitrag die einzelnen Mitgliedsbranchen zum IT-Risiko- und Chancenmanagement beisteuern können.

Des Weiteren stellt als „Gastbranche“ die Versicherung als wichtiger Partner im Bereich IT-RCM ihren Beitrag dar.

5.1 HW/SW-Hersteller

Die HW/SW-Hersteller bieten Produkte an, die sowohl den gesamten IT-RCM-Prozess als auch die Umsetzung der einzuleitenden IT-Sicherheitsmaßnahmen unterstützten. Der Markt ist hier sehr groß und umfasst sehr viele Bereiche im Umfeld IT-Sicherheitsmanagement, sie reichen z.B. vom Anbieter singulärer Firewall-Rechner bis hin zum Lieferanten aller erforderlichen Komponenten zur Erstellung eines abgeschirmten Netzwerks.

Im Bereich der Software-Hersteller gibt es z. B. Anbieter für IT-RCM-Produkte. Hier kann der gesamte Prozess des IT-RCM anhand von Softwareprodukten geführt durchlaufen werden. Einfache Produkte, für kleine überschaubare Unternehmen, werden z. T. auch kostenlos angeboten. Ein anderer Bereich ist die Lieferung von Warninformationen über Sicherheitslücken in Softwareprodukten und dem zur Verfügung stellen von Sicherheitsupdates. Auch Virenschutzprogramme helfen das IT-Risiko zu reduzieren. Natürlich reduziert auch eine Buchhaltungssoftware, die für eine ordnungsgemäße Datenverarbeitung der buchhalterischen Daten sorgt, das IT-Risiko und unterstützt damit das IT-RCM.

5.2 Systemintegration

Systemintegrationen (auch Systemhäuser) spielen bei der Einführung von neuer Hardware oder/und Software im Unternehmen eine Rolle. Bei großen IT-Projekten, die die bestehende IT-Landschaft verändern oder wenn das notwendige Know-how im Unternehmen nicht vorhanden ist, werden Systemintegratoren für das Projektmanagement beauftragt. Sie übernehmen die Generalunternehmerschaft für das IT-Projekt und damit die Verantwortung für das Gelingen des Projektes. Die Projektrisiken (z. B. Lieferzeit, Schnittstellenanpassung, Dokumentation, Softwareentwicklung, Funktionalität) werden vom Unternehmen auf den Systemintegrator übertragen. Aufgrund seiner Erfahrungen und seinem Know-how kann er die Risiken abschätzen, bewerten und gegensteuern.

5.3 Outsourcer/ Provider /ITK-Serviceunternehmen

Ein IT-Betrieb besitzt immer Risiken. Diese Risiken kann ein Unternehmen reduzieren, indem z. B. Teile des IT-Betriebes outgesourct werden. Das Outsourcing kann unterschiedliche Formen annehmen, z. B. Betrieb von Hardware, Auftragsdatenverarbeitung, Langzeitarchivierung von Daten, Betrieb von Software. Beim Outsourcing werden die Risiken an den Outsourcer übergeben, der dafür finanziell entlohnt wird. Der Outsourcer muss sowohl die rechtlichen Anforderungen (z. B. Datenschutz) erfüllen, als auch die Unternehmensanforderungen. Hierfür werden Service-Level-Agreements mit dem Outsourcer vertraglich vereinbart. Der gesamte Outsourcingprozess sollte im Rahmen des IT-RCM überwacht werden.

Ähnliches gilt auch für Telekommunikationsprovider. In der Regel haben Unternehmen ihre gesamte TK auf einen Provider ausgelagert. Auch dieser übernimmt die Risiken für die Sicherstellung der Telekommunikation des Unternehmens in seinem eigenen Netz. Das IT-RCM sollte auch diesen Prozess überwachen.

ITK-Serviceunternehmen bieten die Übernahme von Dienstleistungen z. B. im Bereich Fernwartung, Help-Desk an. Das Unternehmen braucht kein eigenes Know-how aufzubauen. Vertraglich muss vereinbart werden, welche Leistungen das ITK-Serviceunternehmen übernimmt und wie der Zugriff auf die Arbeitsplatzrechner erfolgt. Es sorgt für die Sicherheit der Rechner und reduziert in diesem Bereich die IT-Risiken.

5.4 IT-Berater

Führt ein Unternehmen ein IT-RCM-Prozess ein, so muss das Unternehmen seine wichtigsten Mitarbeiter zunächst schulen und von der täglichen Arbeit z. T. freistellen. IT-Berater können hier unterstützen und wesentliche Prozessschritte verantworten und übernehmen. Der Schulungsaufwand und die Freistellung fällt geringer aus. Insgesamt kann durch den Einsatz von qualifizierten Beratern der zeitliche Aufwand reduziert werden, da diese Verfahrensweisen, Tools, Checklisten usw. kennen und in das Projekt schon einbringen.

Das Risiko bei IT-Projekten kann durch den Einsatz von ausgewählten IT-Beratern reduziert werden. Sie können Projekt- oder auch Qualitätsmanagement Aufgaben übernehmen, sofern das Know-how im eigenen Unternehmen nicht vorhanden ist.

5.5 Wirtschaftsprüfer

Die Bewertung der Sicherheit und Eignung von IT-Systemen in Bereichen, die für die Rechnungslegung von Unternehmen relevant sind, erhält durch die gestiegenen Anforderungen von Banken und Gesetzgeber einen immer höheren Stellenwert in den Abschlussprüfungen der Wirtschaftsprüfungsgesellschaften. Hierbei ist es für das Testat des Wirtschaftsprüfers von besonderem Interesse, die IT-Systeme hinsichtlich der Kriterien "Vertraulichkeit", "Integrität", "Verfügbarkeit",

"Autorisierung" sowie "Verbindlichkeit" zu überprüfen, um somit die Einhaltung der Grundsätze ordnungsgemäßer Buchführung bewerten zu können.

Das Institut der Wirtschaftsprüfer (IDW) hat Empfehlungen ausgesprochen, welche Bereiche der rechnungslegungsrelevanten Datenverarbeitungssysteme in einem Unternehmen besonderer Beachtung hinsichtlich der Grundsätze ordnungsgemäßer Buchführung bedürfen.

Im Rahmen eines freiwilligen IT-Audits wird der Ist-Zustand der rechnungslegungsrelvanten Systeme analysiert, die IT-Infrastruktur, die eingesetzten Anwendungen, die IT-gestützten Geschäftsprozesse sowie das interne Kontrollsystem überprüft. Dabei sind auch die Auswirkungen von Katastrophen auf die bestehende IT-Infrastruktur und die damit verbundenen geschäftskritischen Prozesse zu analysieren. Die Ergebnisse werden in einem ausführlichen Bericht zusammengefasst, der für Systemadministratoren wie Unternehmensleitung Transparenz gewährleistet und im Rahmen der Jahresabschlussprüfung durch den Wirtschaftsprüfer als externes Prüfungsergebnis verwertet werden kann.

5.6 Rechtsanwälte

Der Jurist ist in erster Linie bei allen vertragsrelevanten Vereinbarungen bzw. Änderungsvereinbarungen gefragt. Dieses Fachwissen ist für die Feststellung von rechtlichen Risiken notwendig, die durch Verletzung von vertraglichen Rechten und Pflichten wie zum Beispiel durch unvollständige, schlechte oder verspätet erbrachte Leistungen entstehen. Das vertragliche Risikomanagement umfasst den gesamten Zeitraum der Projektes sowie nachfolgende späteren Wartungs- und Pflegephasen.

Als prüfenswert stellen sich unter anderen Fragen nach der Durchsetzbarkeit von Erfüllungsansprüchen oder nach den finanziellen Auswirkungen von Schadensersatzansprüchen auf die Wirtschaftlichkeit des Projektes.

Die Norm ISO 9001 schreibt nur eine Struktur der Prüfgegenstände vor; sie gibt aber keine inhaltlichen Empfehlungen für die Vertragsgestaltung. Die Qualität eines Produktes sollte entsprechende vertragliche bzw. rechtliche Absicherung gewährleistet werden.

Die juristische Aufgabe ist demnach im Einzelfall nicht nur die Feststellung, ob ein Vertrag alle erforderlichen Regelungen wie Verzug, Abnahme, Meilensteine, Gewährleistung, Haftung enthält, sondern ob der Vertrag ausreichend detailliert und angemessen die Leistungen beschreibt, die erforderlichen Rechte (Nutzung-, Verwertung-, Markenrechte usw.) einräumt und eventuelle Leistungsrisiken angemessen den Vertragspartnern zuordnet. In der Kombination von technischem und rechtlichem Know-how können Entwicklungsrisiken weitgehend effektiv vermieden werden.

Der wirtschaftliche Aufwand des Risikomanagements muss allerdings immer wieder kritisch geprüft werden – er muss angemessen sein! Auch hierbei kann der mit der IT-Branche vertraute

Jurist hilfreich zur Seite stehen: der breite Rahmen spannt sich von der Feststellung des zumutbaren Aufwands für einen Geschäftsführer, um ihn von der persönlichen und ggf. strafrechtlichen Haftung freizuhalten, über die telekommunikations- und betriebsverfassungs-rechtlich zulässigen Maßnahmen zur Abwehr von Spam-Mails, bis hin zur Prüfung der Nutzungserlaubnis lizenz-/urheberrechtlich geschützter Produkte und Leistungen.

Erst aus der Vielzahl der technischen, rechtlichen und finanziellen Analysen ist der Projektstatuts feststellbar sowie Art und Umfang der erforderlichen Entscheidungen über die einzelnen Schritte des Projektes. Dabei können insbes. zahlreiche, unterschiedlich ausgerichtete BITKOM-Mitgliedsunternehmen unterstützende Beiträge leisten.

5.7 Versicherung

Die Risiken, d.h. Chancen und Gefahren bzw. Schäden, die ein Unternehmen beeinflussen, sind sehr vielfältig. Ebenso unterschiedlich sind die Maßnahmen, die ergriffen werden können, um möglichen Gefahren zu begegnen. So könnten denkbare Materialpreisschwankungen durch vertraglich geregelte Preisgleitklauseln an Kunden durchgereicht werden. Lieferantenratings helfen, die Zuverlässigkeit von Lieferanten mit einer Ausfallwahrscheinlichkeit zu beschreiben und somit mögliche Materialengpässe vorherzusehen. Auch die Einrichtung eines Lagers kann als Risikobewältigungsmaßnahme angesehen werden, da mit der Schaffung eines Lagerpuffers Lieferengpässe vermieden werden können. Die mit diesen verschiedenen Maßnahmen einher gehenden Aufwendungen, werden oftmals nur mittelbar als Risikokosten gesehen.

Die bewusster wahrgenommenen und besser quantifizierbaren Risikokosten sind die Versicherungsprämien. Die Versicherung als klassische Risikobewältigungsmaßnahme, findet die vor allem bei operationellen Risiken mit direkter oder indirekter Sachwertreduzierung Anwendung. Eine Versicherung stellt hierbei für das versicherte Unternehmen eine kollektive, externe Risikoreservebildung (im Gegensatz zur individuellen, unternehmensinternen Risikofinanzierung) dar . Die grundlegende Idee der Versicherung ist der gegenseitige Schutz Einzelner im Kollektiv. Der Kern des Versicherungsgeschäftes ist der entgeltliche Transfer von Risiken auf eine große Gesamtheit, wobei mittels Diversifikationseffekte des Portfolios das Gesamtrisiko reduziert werden kann.

Neben dem reinen Risikotransfer spielt die Beratung zur Schadenverhütung eine weitere große Rolle im Kerngeschäft der namhaften Firmen- und Industrieversicherer. Unter Mitwirkung und Informationsbereitstellung des Kunden, können Handlungsempfehlungen zur Optimierung seines Risikos erarbeitet werden. Solche Schadenverhütungsmaßnahmen tragen i.d.R. deutlich zur Reduzierung des betroffenen Risikos bei und nutzen dem Kunden und dem Versicherer. Vor der Schadenverhütung steht die Beurteilung von IT-Risiken. Eine besondere Herausforderung stellen hierbei die Komplexität und Vernetzung der Systeme dar, was nur mit aufwändigen technischen und ökonomischen Risikoanalysen bewältigt werden kann. Sind die Gefahrenquellen erst identifiziert, gibt es eine breite Palette an Versicherungslösungen, die stets für den individuell zu betrachtenden Fall zu kombinieren und anzupassen sind. Für jedes Produkt sind die versicherte Sache, die

versicherte Gefahr und die eigentliche Versicherungsleistung zu unterscheiden. So kann beispielhaft folgende Aufstellung gemacht werden, wobei für jeden betrachteten Einzelfall unterschiedliche Sachen, Gefahren und Leistungen definiert sein können:

- **Elektronikversicherung**
  - Versicherte Sachen: Anlagen und Geräte der Informations-, Kommunikations- oder Medizintechnik, nicht auswechselbare Datenträger, Daten für Grundfunktionen (Betriebssystem)
  - Versicherte Gefahren: Unvorhergesehene Ereignisse wie z.B. Bedienungsfehler, Ungeschicklichkeit, Fahrlässigkeit, Induktion, Wasser, Brand, Sabotage, Konstruktionsfehler, etc.
  - Versicherungsleistung: Im Totalschadenfall wird der Neuwert ersetzt. Bei zerstörten oder abhanden gekommenen Sachen die Wiederbeschaffung neuer Sachen gleicher Art und Güte.
- **Datenträgerversicherung**
  - Versicherte Sachen: Auswechselbare Datenträger sowie Daten aus serienmäßig hergestellten Standardprogrammen
  - Versicherte Gefahren: Schäden an Daten durch einen Sachschaden am Datenträger oder der verarbeitenden Anlage sowie durch Blitzeinwirkung
  - Versicherungsleistung: Wiederbeschaffung, Wiedereingabe oder Wiederherstellung von Stamm- und Bewegungsdaten; Wiederbeschaffungskosten für Datenträger.
- **Feuerversicherung**
  - Versicherte Sachen: Gebäude, Inventar, Vorräte
  - Versicherte Gefahren: Brand, Blitzschlag, Explosion, Anprall oder Absturz eines Flugkörpers
  - Versicherungsleistung: Entschädigt werden Gebäude-, Sach-, und Inventarswerte
- **Betriebsunterbrechungsversicherung**
  - Versicherte Sachen: Gehaftet wird für den Unterbrechungsschaden, der innerhalb der vereinbarten Zeit, seit Eintritt des Sachschadens entsteht.
  - Versicherte Gefahren: Betriebsunterbrechung aufgrund eines Sachschadens. (Mögliche Gefahren siehe Elektronikversicherung)
  - Versicherungsleistung: Betriebsgewinn und fortlaufende Kosten = Deckungsbeitrag
- **Betriebshaftpflichtversicherung**
  - Versicherte Sachen: Die Versicherung umfasst die Deckung von Sach-, Personen- oder Vermögensschäden bei Dritten, die gegen den Versicherungsnehmer bei Ausübung einer

beruflichen Tätigkeit von ihm selbst oder einer Person, für die er einzutreten hat, geltend gemacht werden.

- Versicherte Gefahren: Verstoß bei beruflicher Tätigkeit, auf Grund deren ein Anspruch aus der gesetzlichen Haftpflichtbestimmung privatrechtlichen Inhalts entsteht.
- Versicherungsleistung: Haftpflichtansprüche Dritter sowie die Abwehr unberechtigter Ansprüche.

Zu beachten ist in diesem Zusammenhang, dass das Versicherungsunternehmen im Rahmen seines eigenen Risikomanagements bestrebt ist, die versicherten Risiken zu minimieren. Deswegen kann der Versicherungsschutz mit Auflagen verbunden sein (Obliegenheiten), die i.d.R. zu einer deutlichen Gefahrenreduzierung beim Versicherungsnehmer führen können. Solche empfohlenen und teilweise geforderten Schadenverhütungsmaßnahmen sind z.B. im Merkblatt zur Schadenverhütung "Anlagen der Informationstechnologie" VdS 2007 aufgeführt. Der Versicherer kann hierbei die Prämie reduzieren, falls besondere zusätzliche IT-Risikobewältigungsmaßnahmen ergriffen werden. Beispiele hierfür sind: Brandwände und Komplextrennungen, automatische Brandmelde- und Löschanlagen, überwachte redundante Energieversorgung und Datenleitungen, regelmäßige Datensicherung, Überspannungsschutz, etc. Hier wird deutlich, dass neben dem Erhalt der Geschäftsfähigkeit auch ein gewisser finanzieller Vorteil mit der Einrichtung eines IT-RCM bzw. dem Umsetzen von Bewältigungsmaßnahmen einher gehen kann.

Firmen- und Industrieversicherer, die sich intensiv mit vorbeugender Schadenverhütung befassen, sind daher als strategische Partner zu verstehen, die ebenfalls Interesse an der Implementierung, bzw. an der Verbesserung eines bereits bestehenden systematischen Risikomanagementsystems haben: Dies unterstützten sie mittels Beratungen und Empfehlungen zur Schadenverhütung unter Ausnutzung der bei ihnen gebündelten Schadenerfahrung. Weil aber IT-Risiken nur ein Teilaspekt einer ganzheitlichen Risikobetrachtung sind, bieten einzelne Versicherungsgesellschaften auch Risikomanagement-Beratungsdienstleistungen in eben diesen übergeordneten Unternehmensbereichen an. Hierzu gehören die Strategie, der Markt, der Finanzmarkt, die politisch, rechtlich, gesellschaftlichen Bereiche, die Unternehmenskultur und -organisation sowie die komplette unternehmensspezifische Leistungserstellung mit allen zugehörigen Unterstützungsprozessen. Erst unter Einbeziehung dieser gesamtunternehmerischen Teilbereiche, deren Risiken u.U. gar nicht versicherbar sind, kann die Tragweite von IT-Risiken korrekt abgeschätzt und eine Gesamtrisikoposition des Unternehmens ermittelt werden. Dies ist bei der Analyse und Bewertung von IT-Risiken stets zu beachten.

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.000 Unternehmen, davon 750 Direktmitglieder mit etwa 120 Miliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Geräte-Hersteller, Anbieter von Software, IT-Services, Telekommunikationsdiensten und Content. Der BITKOM setzt sich insbesondere für bessere ordnungsrechtliche Rahmenbedingungen, eine Modernisierung des Bildungssystems und eine innvationsorientierte Wirtschaftspolitik ein.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.
Albrechtstraße 10
10117 Berlin

Tel.: 030/27 576-0
Fax: 030/27 576-400

www.bitkom.org
bitkom@bitkom.org