September 2001

IT Risk Management - Fit für E-Business?

Markus Junginger
Universität Hohenheim, markjung@uni-hohenheim.de

Helmut Krcmar
Universität Hohenheim, krcmar@uni-hohenheim.de

In: Buhl, Hans Ulrich, u.a. (Hg.) 2001. *Information Age Economy*; 5. Internationale Tagung Wirtschaftsinformatik 2001. Heidelberg: Physica-Verlag

ISBN: 3-7908-1427-X

IT Risk Management – Fit für E-Business?

Markus Junginger, Helmut Krcmar
Universität Hohenheim

Zusammenfassung: E-Business Risk ist eine Kombination von Geschäftsmodell und Technologie. Gegenstand eines effektiven und effizienten IT-Risk Managements ist folglich die Verbindung von Geschäftsmodell und Technologie. Es wird als Gesamtheit aller Maßnahmen, Prozesse und Institutionen verstanden, die auf eine zielgerichtete Gestaltung der vom Informationsmanagement ausgehenden Gefährdungen auf die Geschäftsprozesse und Gesamtrisikolage des Wirtschaftssubjektes ausgerichtet sind. Neben den technologischen Einzelrisiken von Seiten der Informationsverarbeitung bedrohen von Seiten der Informationsverwendung Informationspathologien und eine unzureichende strategische Orientierung die Wettbewerbsfähigkeit der Unternehmung nachhaltig. Bekannte Konzepte im Bereich des IT-Risk Managements wie beispielsweise das IT-Grundschutzhandbuch, die Common Criteria, oder das V-Modell in der Software-Entwicklung konzentrieren sich lediglich auf Teilbereiche der Risiken des Informationsmanagements. Zur Überwindung der in dieser Arbeit aufgezeigten Führungslücke im IT-Risk Management wird die Entwicklung eines ganzheitlichen Modells vorgeschlagen, das Portfolio-, Projekt-, Produkt-, Integrations- und Überwachungs-Risiken angemessen berücksichtigt.

Schlüsselworte: Risikomanagement, Informationsmanagement, IT-Risk Management, E-Business, KonTraG, IT-Security, Datensicherheit.

1 Einleitung

1.1 Informationstechnologie – Enabler und Risikofaktor

Wurde das Risikomanagement von Informationssystemen auf Ebene der Unternehmensführung lange Zeit unter Kostengesichtspunkten betrachtet, so kann in jüngster Zeit ein „boardroom breakthrough“ festgestellt werden, der zur Aufmerksamkeit des Vorstandes und des Top-Managements für diese Problematik führt. Die Gründe für den Durchbruch sind in der Beachtung der zukünftigen Chancen des Electronic-Business (E-Business), dessen Grundlage ein zuverlässiges IT-Konzept für Partner und Kunden ist, zu finden [InSe99]. Ein weiterer Aspekt, der das Augenmerk des Managements auf die Sicherheit, Zuverlässigkeit und Integri-

tät der betrieblichen Datenverarbeitung lenkt, ist die internationale Corporate Governance Debatte, die in der Bundesrepublik Deutschland 1998 mit der Verabschiedung des Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) ihren vorläufigen Höhepunkt erreicht hat. Als wesentliche Neuerung wird hier die Einrichtung eines Risikofrüherkennungs- und Überwachungssystems gefordert, um den Fortbestand der Gesellschaft gefährdende Entwicklungen frühzeitig erkennen zu können [HoMa98]. Der oftmals in diesem Kontext diskutierte Teilaspekt der IT-Sicherheit – der Sicherstellung der Daten- und Systemsicherheit auf technologischer Ebene – erscheint kein ausreichender Ansatz zu sein.

Diese Arbeit beschäftigt sich mit existierenden Konzepten und der systematischen Realisation eines IT-Risk Managements. Es wird geprüft, inwieweit bisher bekannte Ansätze aus Sicht eines ganzheitlichen Informationsmanagements (IM), insbesondere unter der Berücksichtigung der Gefährdungen des E-Business, die Identifikation und Steuerung aller damit verbundenen Risiken sicherstellen können. IT-Risk Management (ITRM) beinhaltet hierbei die Gesamtheit aller Maßnahmen, Prozesse und Institutionen, welche auf eine zielgerichtete Gestaltung der vom Informationsmanagement ausgehenden Gefährdungen und Risiken auf die Geschäftsprozesse und Gesamtrisikolage des Wirtschaftssubjektes ausgerichtet sind [Boeh89; Fass95; Kend98; Pali01].

1.2 IT-Risiken – Risk Driver E-Business?

Jede Entscheidung für den Einsatz eines Informationssystems oder einer Informationstechnologie bietet die Chance zur Eröffnung neuer organisatorischer Spielräume. Damit nimmt jedoch auch die Abhängigkeit der Prozesse von der Angemessenheit, Sicherheit und Qualität der eingesetzten Systeme und Technologien in erheblichem Maße zu und stellt für ein funktionsfähiges Informationsmanagement ein Risiko[1] dar. Die zunehmende Nutzung der Potenziale des E-Business, was in dieser Arbeit als elektronische Integration wertschöpfungskettenübergreifender Prozesse (E-Integration) verstanden wird, stellt eine neue Herausforderung an das Informationsmanagement dar. Der bisherige Fokus des IT-Risk Managements lag bei der Bewältigung der Gefährdungen für die unternehmensinterne Informationsversorgung. Dieser weitet sich um die Risikobewältigung bezüglich der Integration der eigenen Geschäftprozesse in wertschöpfungsketten- und organisationsübergreifende elektronische Koordinationsformen aus.

In Anlehnung an das Ebenenmodell des IM nach Krcmar [Krcm00] können anhand der Aufgaben des IM[2] grundsätzliche Risikopotentiale abgeleitet werden.

---

1 Das Risiko wird als Gefahr der Zielabweichung des realisierten Ergebnisses vom Sollzustand verstanden [Brau84].

2 Die Aufgaben des IM können unterschieden werden in die Ebenen Management der Informationstechnologien, Management der Informationssysteme, Management der

Hierbei können zu jeder Ebene des Informationsmanagements spezifische Risiken zugeordnet werden. Die Wirkung zeigt sich in Informationspathologien[3], Prozessdisfunktionalitäten, unzureichender Verfügbarkeit von Technologien und einer mangelnden Strategieorientierung. Das Ergebnis ist eine Nichterfüllung der Ziele des IM und daraus resultierend eine mangelnde Wettbewerbsfähigkeit des Unternehmens. Die einzelnen Risiken sind nicht isoliert, sondern haben interdependente Ausstrahlungswirkungen auf die Risiken anderer Ebenen. So können Prozessdisfunktionalitäten, die primär auf Ebene der Informationssysteme ihre Ursachen haben, auch durch mangelnde Verfügbarkeit, beispielsweise von Rechenkapazitäten auf Ebene der Informationstechnologien, induziert werden.

Aus Sicht eines effizienten IT-Risk Managements stellt sich die Frage, welche zusätzlichen Risiken sich aus der zunehmenden E-Integration ergeben. Hier wird die These vertreten, dass sich das technologieinduzierte Risikopotenzial exponiert. Hierfür können zwei Gründe angeführt werden. Zum einen sind mit der geeigneten Unterstützung der Marktprozesse durch E-Business für das Unternehmen erhebliche Erwartungen bezüglich Effektivitäts- und Effizienzsteigerungen in der Kunden-Lieferanten-Beziehung (KLB) verbunden. An den Schnittstellen des Unternehmens werden zum anderen klassische Kontrollmechanismen außer Kraft gesetzt. So war die KLB nach außen bisher durch persönliche Kontakte oder manuelle Eingaben und Kontrollen durch eine lose Kopplung der internen und externen Informationssysteme gekennzeichnet. Schwächen in der eigenen Informationsverarbeitung, sowohl auf Ebene der Informationsverarbeitung als auch der Informationsverwendung, konnten durch individuelles Engagement ausgeglichen werden. Etwa durch Vertriebsbeauftragte, die bei der unzureichenden Erläuterung einer Produktbeschreibung das Informationsdefizit des Einkäufers leicht aufklären konnte. Die Zwischenschaltung von Intermediären, welche Unzulänglichkeiten der internen Informationsversorgung, beispielsweise bezüglich der Qualität von Informationen, aufgrund der losen Kopplung leicht abzufedern verstanden, entfällt.

2 Ansätze des IT-Risk Managements

Am Beispiel ausgewählter Methoden und Konzepte aus dem Bereich des IT-Risk Managements und verwandter Gebiete wird dargestellt, inwieweit das Management von IT-Risiken im Sinne der in Kapitel 1.1 getroffenen Definition des ITRM

Informationswirtschaft und Führungsaufgaben des Informationsmanagements [Krcm00].

[3] Informationspathologien sind Fehlfunktionen in der organisatorischen Wissensverarbeitung und beeinflussen den Erfolg der Gewinnung, Weitergabe und Verwendung von Informationen [Scho92].

unterstützt wird. Tabelle 1 gibt einen Überblick über die wichtigsten, gängig genutzten Ansätze des ITRM und die Problematik dieser Konzepte, besonders vor dem Hintergrund des E-Business.

Methode	Unterstützung des IT-Risk Managements im Ebenenmodell				*Bemerkungen*
	Führungsaufgaben	Informationswirtschaft	Informationssysteme	Informationstechnologien	
IT-Grundschutzhandbuch (GSHB) [BuSi99]	☑	O	☑	☑	komplex, technologieorientiert, Fokus Einzelorganisation
Informationssicherheit in der Bürokommunikation [Voßb93]	O	O	☑	☑	keine Berücksichtigung der strategischen Dimension, Fokus Einzelorganisation
Common Criteria (ISO 15408) [CoCr01]	O	O	☑	☑	Zertifizierungsrichtlinien, fördern Vertrauen und Vergleichbarkeit
Control Objectives for Information and Related Technology (COBIT) [ISAC00]	☑	☐	☑	☑	ganzheitlich, abstrakt, Schwerpunkt Revision, Soll-Prozesse
Spiralmodell [Boeh89]	O	O	☑	O	nur in der Anwendungsentwicklung relevant
V-Modell [Balz98]	O	O	☑	O	nur in der Anwendungsentwicklung relevant
IS-Portfolio [KrBu94]	O	O	☑	O	nur für IS-Planung relevant
Legende:	☑ Unterstützung		☐ bedingte Unterstützung		O keine Unterstützung

Tabelle 1: Konzepte des ITRM

Im Zuge eines Vergleichs der Reichweite der einzelnen Methoden werden die Aufgaben des Informationsmanagements in Anlehnung an das Ebenenmodell von Krcmar [Krcm00] als Referenz herangezogen. In Tabelle 1 werden die Unterstützungspotenziale der einzelnen Konzepte bei der Bewältigung der spezifischen Aufgabenrisiken verglichen. Die nicht berücksichtigten Aufgabenfelder sind grau unterlegt.

Im Sinne einer Lückenanalyse [Mach99] kann für das Informationsmanagement eine Führungslücke attestiert werden. Die vorhandenen Konzepte und Methoden des Risk Managements wurden nicht für das Management strategischer Risiken und der Risiken der Informationswirtschaft konzipiert. Problematisch ist dies im

Hinblick auf die strategische Bedeutung des Informationstechnologieeinsatzes sowie der damit verbundenen Notwendigkeit einer Integration des IT-Risk Managements in das strategische Risk Management des Unternehmens. Erfährt ein umfassendes Risk Management auf der Modellebene der Informationstechnologien durch existierende Konzepte noch eine hinreichende Unterstützung, so wird bereits beim Management der Informationssysteme eine unzureichende Leistungsfähigkeit deutlich. Hier ist das Risikopotenzial besonders durch Prozessdisfunktionalitäten gekennzeichnet. Eine ebenso ungenügende Unterstützung erfahren die inhärenten Risiken auf der Beschreibungsebene des Managements der Informationswirtschaft. In Bezug auf spezifische Risiken des E-Business ist zu kritisieren, dass meist der Fokus der Einzelorganisation im Vordergrund steht. E-Business spezifische Risiken, die sich aus der zwischenbetrieblichen Vernetzung ergeben, werden einzig aus technologischer Sicht betrachtet, wie beispielsweise beim IT-Grundschutzhandbuch bei der Frage nach der eigenen Internet-Security. Hervorzuheben sind die Common Criteria, die bei einer Zertifizierung zwischen Partnern Vertrauen und Vergleichbarkeit schaffen, jedoch ebenfalls schwerpunktmäßig auf technologischer Ebene.

3 Ein prozessorientierter Modellrahmen für das IT-Risk Management

3.1 Ein Modell des IT-Risk Managements

Im Verständnis einer Kunden-Lieferanten-Beziehung zwischen Geschäftsprozessen und der Unterstützungs- und Enabler-funktion des Informationsmanagements, ist die Frage nach der zu erbringenden Dienstleistung des IM für die effiziente Abwicklung des Prozesses entscheidend. Jedes Handeln des Informationsmanagements im Rahmen eines IM-Prozesses, wird aus Sicht des IT-Risk Managements als Risikoobjekt verstanden.

Einen Ansatz für eine prozessorientierte Sicht auf das Management von IT-Risiken bietet das Konzept des IV-Controlling [KrBu94]. Der Lebenszyklus für die Ressourcen des IM – Personal, Software, Hardware und Information – besteht aus den Phasen Portfolio-, Projekt-, sowie Produkt- und Infrastrukturmanagement. Die prozessorientierte Sichtweise wird darüber hinaus, basierend auf dem idealtypischen Managementzyklus, um die Phase der Kontrolle [Hein91] erweitert, die zur Überprüfung der Wirksamkeit aller Maßnahmen des ITRM notwendig ist. Die Aufnahme der Kontrolle stellt vor dem Hintergrund der Forderung des KonTraG nach der Errichtung eines Überwachungssystems für das Risikomanagement die Konsistenz des Modells mit gesetzlichen Rahmenbedingungen sicher [Lück98].

In Anlehnung an die Phasen des oben dargestellten Zyklus werden die Risikofelder des IT-Risk Managements identifiziert. Hierbei wird die Sicht des Infrastrukturmanagements erweitert und als Management der Integration sowohl in intra- als auch interorganisationale Prozesse verstanden [ScKr94]. Es ergibt sich das in Abbildung 1 dargestellte Modell. Es besteht aus dem generischen Risikozyklus, den mit allen Risikofeldern korrespondierenden Integrations-Risiken im Zentrum, und dem äußeren Zyklus des Überwachungs-Risikos.

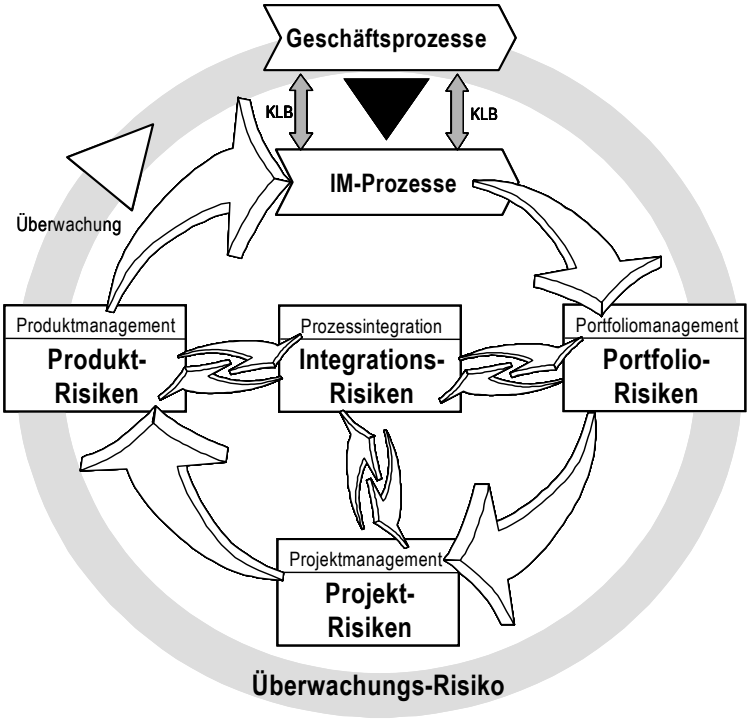

Abbildung 1: Ein Modell des IT-Risk Managements

Während die Risikoobjekte, also die prozessspezifischen Aufgaben des IM, den Zyklus aus den Phasen Portfolio-, Projekt- und Produktmanagement durchlaufen, ist das Integrationsrisiko als Querschnittsrisiko bei allen Phasen des Zyklus präsent. Das Risikoobjekt steht zwar den spezifischen Risiken der Risikofelder gegenüber, gleichzeitig korrespondiert es auch im Umweltkontext mit anderen IM-Prozessen, der gesamten Unternehmensumwelt sowie zwischenbetrieblichen Kooperationen. So wird insbesondere der aus Sicht des E-Business relevante interorganisationale Umweltkontext gewahrt.

Der dargestellte Ansatz erlaubt die besondere Berücksichtigung der Anforderungen kritischer Geschäftsprozesse und ermöglicht dem ITRM, durch gezielte Fo-

kussierungen Schwerpunkte zu bilden. Ausgehend von einer Prozessrisikoanalyse wird das IT-spezifische Risiko im Rahmen des ITRM identifiziert, analysiert und gesteuert. Dadurch wird auch die Schnittstelle zum integrierten unternehmensweiten Risk Management deutlich. Der Zyklus erlaubt es zudem, die sich gegenwärtig stark ändernden Aufgaben des IM angemessen zu berücksichtigen. Standen bei der bisherigen Betrachtung die unternehmensinterne Informationsversorgung im Vordergrund, so liegt der Fokus des E-Business auf der zwischenbetrieblichen Ebene bzw. an der Schnittstelle zum Kunden.

3.2 Risikofelder und Risikoursachen

Durch welche Merkmale sind die einzelnen Risikofelder gekennzeichnet und welche Ursachen führen zu diesen Risiken? Es ist zu klären, welchen Handlungsrisiken die Risikoobjekte in den einzelnen Phasen ausgesetzt sind und welche Ursachen für diese Risiken verantwortlich sind.

Portfolio-Risiken sind gekennzeichnet von Risiken, die im Management der Ideen und Planung des IM begründet sind. Besondere Risikopotenziale liegen in der Bewertung von Nutzen und Risiko sowie bei der Strategieorientierung und Infrastrukturorientierung einer Handlungsalternative. Fehlanalysen bei der Bewertung der Chancen des E-Business und der Auswahl von Plattformen in dieser Phase können langfristige Folgen haben. In späteren Phasen des Zyklus schlägt sich dies in mangelnder Effizienz und Effektivität nieder.

Projekt-Risiken entstehen durch Probleme und Gefahren bei der Projektabwicklung. Im Rahmen des Projektmanagements stehen das Management der Termine, Kosten, Ressourcen, die Abschätzung des Aufwands und die Koordination der Vorgänge im Vordergrund [Hein91]. Viele E-Business Projekte werden unter hohem Zeitdruck realisiert, wovon sich viele Marktteilnehmer die Mitnahme von „first mover advantages“ versprechen. Die Aufgabe des ITRM ist es hier, die Berücksichtigung der Zielgrößen Funktionalität, Qualität und Kosten sicherzustellen, um eine langfristige Wirtschaftlichkeit nicht zu gefährden.

Die effiziente und effektive Nutzung eines Handlungsobjekts in der Phase des Produktmanagements ist durch **Produkt-Risiken** gefährdet. Das generelle Ziel während des Einsatzes bzw. der Verwendung von IS ist die Sicherstellung der Wirtschaftlichkeit des Handelns. Die Gefahren sind in einer inadäquaten Erfüllung der Aufgaben der Betreuung, der Wartung von Systemen, der Weiterentwicklung und unter dem Fokus E-Business vor allem der IT-Sicherheit begründet.

Integrations-Risiken erwachsen aus der Gesamtarchitektur der Informationssysteme und Technologien sowie aus der Gesamtheit aller Maßnahmen des IM. Jedes Risikoobjekt muss nicht nur auf sein spezifisches Optimum ausgerichtet sein, sondern auch im Hinblick auf seine Eingliederung und Übereinstimmung mit der bestehenden und zukünftigen E-Business Strategie sowie der Unternehmensar-

chitektur und dem Umweltkontext beurteilt werden. Kennzeichnend ist der Querschnittscharakter dieses Risikofeldes. Jedes einzelne Risikofeld steht diesem Risiko gegenüber. Das einzelne Objekt muss bei allen Maßnahmen auch auf die Übereinstimmung mit der Infrastruktur des Handlungsumfeldes geprüft werden. Mangelnde Prozess- und Strategieorientierung, ungenügende Kontrolle der Leistungsfähigkeit und Wirtschaftlichkeit eines Bausteins gefährden den Erfolg der Gesamtumwelt.

Das **Überwachungs-Risiko** ist in den Überwachungstätigkeiten über das IT-Risk Management begründet. Die reine Existenz eines ITRM darf ein Unternehmen nicht in vermeintliche Sicherheit wiegen, sondern muss selbst einer ständigen Kontrolle und Prüfung auf Angemessenheit und Funktionsfähigkeit unterworfen werden. Daher ist das Ziel der Überwachung eine ständige Kontrolle und Prüfung des ITRM auf die Angemessenheit und Effizienz des Systems.

Welchen Vorteil hat diese abstrakte und allgemeine Darstellung des ITRM? Zunächst einmal ist der ganzheitliche Charakter des Modellrahmens hervorzuheben. Jedes Handlungsobjekt, sei es der Einsatz von Technologiebündeln auf der Ebene des Managements der Informationstechnologien oder die Strategiefestlegung, kann diesem Zyklus unterworfen werden. Der spezifische Risikocharakter eines jeden Risikoobjekts kann somit individuell auf seine Ursachen hin untersucht und bewertet werden, ohne dass hierbei der Zusammenhang zum Geschäftsmodell [Timm98] und zur Umweltintegration verloren geht.

3.3 Risikomanagement-Prozess

3.3.1 Risikoidentifikation und Risikoanalyse

Ziel der Risikoidentifikation ist die strukturierte Erfassung der wesentlichen Risiken des Informationsmanagements. In Anbetracht der Forderungen des KonTraG, bestandsgefährdende Risiken im Lagebericht darzustellen, scheint ein top-down Vorgehen, ergänzt um bottom-up Analysen, geeignet [GlKö99]. Abbildung 2 verdeutlicht diesen Ansatz. Auf Basis einer Identifikation kritischer Geschäftsprozesse in Bezug auf das Geschäftsmodell, beispielsweise unter Zuhilfenahme des Konzepts der Kritischen Erfolgsfaktoren nach Rockart [Rock79], werden die korrespondierenden IM-Prozesse identifiziert. Diese IM-Prozesse werden anhand der Aufgaben des Informationsmanagements in ihre Einzelaufgaben zerlegt, was gleichzeitig als einzelnes Risikoobjekt verstanden wird. Grundsätzlich bleibt über die Betrachtung des Integrationsrisikos auf Ebene der Risikoobjekte immer der Kontext zum gesamten IM-Prozess gewahrt. Ein Beispielszenario aus dem Bereich des E-Business könnte die Einbindung von Endhändlern in einem Vertriebsinformations- und Bestellsystem mit integriertem Konfigurator in der Automobilbranche sein. Im Rahmen des IM-Prozesses können exemplarisch die Aufgaben und somit die Risikoobjekte Kommunikation über das Internet auf Ebene der In-

formationstechnologien, ein mit mySAP.com realisiertes Portal auf Ebene der Informationssysteme oder auf Führungsebene die strategische Behandlung des Prozesses als Waffe [Krcm00] genannt werden. Bezugnehmend auf diese Risikoobjekte können mögliche Risiken unter Zuhilfenahme gebräuchlicher Verfahren wie Checklisten, Simulationen, Nutzwertanalysen oder Szenario-Analysen identifiziert werden. Auch liefern hier etablierte Methoden des ITRM einen wichtigen Beitrag, beispielsweise das GSHB auf Ebene der Informationstechnologien oder die Referenzprozesse des COBIT-Modells auf der Führungsebene.

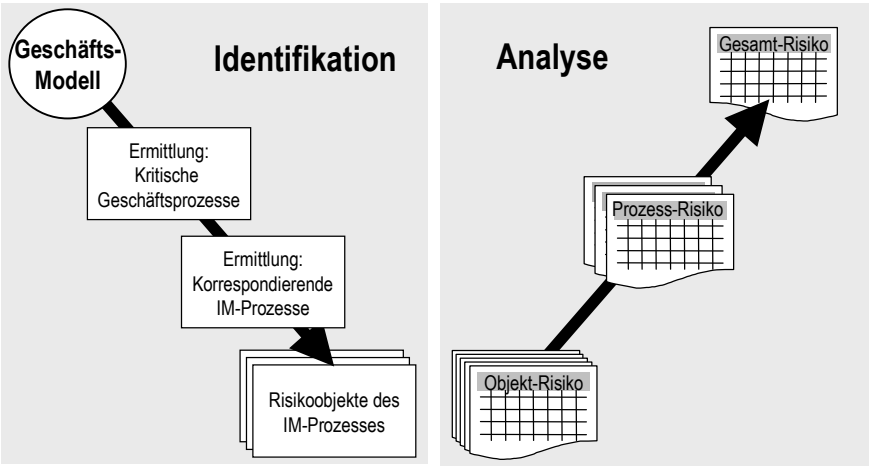

Abbildung 2: Vorgehensmodell zur Risikoidentifikation und -analyse

Ziel der Risikoanalyse ist eine qualitative Bewertung bzw. quantitative Messung der Risiken. Hierbei werden konkrete Ursache-Wirkungs-Beziehungen in Form von Kausalanalysen durchgeführt [Fass95]. Der Einsatz einfacher Schätzungen und Barwertberechnungen ist genauso denkbar wie komplexe Modelle der Fuzzy-Logik [Chor92]. Eine besonders weit verbreitete Methode zur Risikobewertung ist die Value-at-Risk-(VAR-)Methode [Stud98], die aussagt, mit welcher Wahrscheinlichkeit eine bestimmte Verlustgrenze in einer festgelegten Periode nicht überschritten wird.

Kritische Verlustgrenzen, die zeitliche Bewertung von Risikowirkungen und ein angestrebtes Konfidenzniveau des Risikos sind Ergebnis einer organisationsindividuellen Risikostrategiebildung. Die Bewertung der Risikowirkungen erfolgt hier vereinfachend mit verbalen Ausdrücken der Umgangssprache. Der Einsatz numerischer Werte spielt eine scheinbare Genauigkeit vor und birgt eine immanente Ungenauigkeit und Unbestimmtheit in sich. Der qualitative Risikowert dagegen ist von einem Menschen intuitiv einfacher und schneller zu erfassen als der quantitative Wert [Klet93]. Besonders im Rahmen des IT-Risk Managements ist dieser Ansatz praktikabel, da sich die quantitative Ermittlung von Schadenswirkungen, beispielsweise im Vergleich zu den Auswirkungen eines misslungenen Anlagege-

schäftes, als besonders schwierig erweist. Die Wahrscheinlichkeit des Auftretens einer Bedrohung wird mit ihrer **Eintrittsplausibilität** bewertet. Die **Schadenshöhe** wird qualitativ mit linguistischen Termen beschrieben.

Die Ergebnisse dieser Bewertung der Risikoobjekte ermöglichen den Übertrag in ein Risikoportfolio, dessen Felder Auskunft über den Risikowert geben. Durch die Zusammenfassung einzelner Risikoobjekte ist eine Abbildung des Prozessrisikos sowie auf höherer Aggregationsebene auch des Geschäftsmodellrisikos möglich. Diese Darstellung bietet zugleich Anhaltspunkte für die Risikosteuerung. Wie in Abbildung 3 dargestellt muss das Ziel der Maßnahmenbündel eine Clusterung der Objektrisiken eines Prozesses auf dem gewünschten Risikoniveau sein.[4]

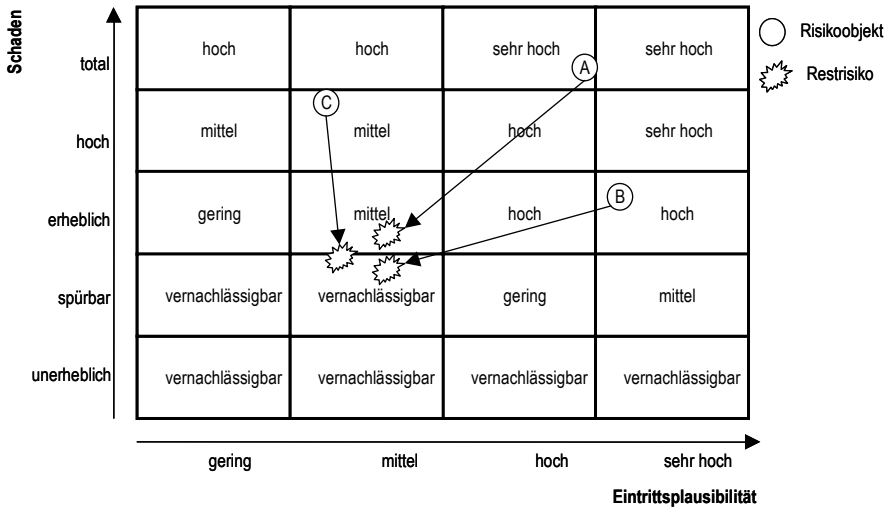

Abbildung 3: Risikoportfolio und Risikowirkungen

3.3.2 Risikosteuerung und Überwachung

Die aktive Beeinflussung der im Rahmen der Risikoanalyse ermittelten Risikopositionen ist Gegenstand der Risikosteuerung. Diese muss in Einklang mit den Unternehmenszielen, der festgelegten Risikopolitik und dem angestrebten Sicherheitsziel stehen. Die Steuerungsmaßnahmen [Fass95] setzen am ursachenbezogenen und wirkungsbezogenen Aspekt des Risikos an. Beim Einsatz des in Abbil-

[4] Für das gewählte Beispiel der Endhändleranbindung mit einer E-Business Lösung in der Automobilindustrie kann das im Portfolio abgetragene Risikoobjekt B herangezogen werden. Es beschreibt die Gefahr der Manipulation der Anwendung mit direktem Einfluss auf die Produktionsplanung durch unsichere lokale Netze bei den Händlern.

dung 3 dargestellten Risikoportfolios kann einerseits Einfluss auf die Eintrittsplausibilität genommen werden, d.h. es findet eine horizontale Verschiebung der Risikoposition eines Objektes statt. Andererseits kann auf eine Verringerung des Schadens abgezielt werden, d.h. es findet eine vertikale Verschiebung des Risikoobjektes statt. Hierzu steht das Instrumentarium des Risk Managements zur Verfügung. Einen Überblick hierüber gibt Tabelle 2.

Risikopolitisches Instrument	Maßnahmen	Anwendungsbereiche
Risikovermeidung	Extremfall der Risikoreduktion auf ein Restrisiko von Null, bspw. Abschaffung eines Systems, Abbruch des Projekts	Vorwiegend bei Risikoeinstufung „sehr hoch“ oder „hoch“
Risikoverminderung	Reduktion der Eintrittsplausibilität und Verringerung der Schadenswirkungen, aktive Beeinflussung der Ursachen sowie antizipatives Handeln des IM	Vorwiegend bei Risikoeinstufung „hoch“ oder „mittel“
Risikoüberwälzung	Übertragung möglicher Störungen vor ihrem Eintritt auf andere Wirtschaftssubjekte, bspw. Outsourcing oder Versicherung	Anwendung bei allen Risikoeinstufungen möglich. Beschränkung meist auf reine Risiken (bspw. Betriebsrisiken im Rechenzentrum)
Risikoselbsttragung	Bewusste Akzeptanz des (Rest-) Risikos, im Rahmen unternehmerischen Handelns nicht eliminierbar, ggf. Bildung von finanziellen oder materiellen Reserven	Management des akzeptierten Restrisikoniveaus („niedrig“, „vernachlässigbar“) nach erfolgter Risikosteuerung
Risikostreuung	Obenstehende Instrumente werden im Rahmen eines Instrumenten-Mixes eingesetzt	Unterstützendes Instrument beim Einsatz aller anderen Risk Management Instrumente

Tabelle 2: Risikopolitisches Instrumentarium

Die Wirkung der Steuerung wird im Risikoportfolio durch die Veränderung der Lage eines Risikoobjektes deutlich. Aus ökonomischer Sicht ist dasjenige Maßnahmenbündel zu ergreifen, bei dem die Grenzkosten gleich dem Grenznutzen der Sicherheit sind. Hierbei spiegelt sich der Nutzen in der Erreichung eines bestimmten Sicherheitsniveaus wider, während die Risikobewältigungsmaßnahmen zu gewinnmindernden Kosten führen [Farn79]. Daraus ergibt sich für das IT-Risk Management ein Dilemma: Während die Kosten sofort messbar sind, ist der Zuwachs an Sicherheit nur sehr schwer quantifizierbar.

Das durch die Risikosteuerung erreichte Restrisikoniveau darf bei den folgenden Aktivitäten des ITRM nicht vernachlässigt werden. Im Rahmen einer ständigen Überwachung müssen die Wirksamkeit aller getroffenen Maßnahmen sowie etwaige Veränderungen der Risikolage ständig kontrolliert und beobachtet werden. Dieser Aspekt ist für ein effizientes IT-Risk Management vor dem Hintergrund von Technologiesprüngen und unvorhergesehenen Entwicklungen im Systemle-

benszyklus von Bedeutung. Im E-Business sind jedoch bei einer wachsenden zwischenbetrieblichen Integration klassische Instrumente wie die interne Revision äußerst problematisch. Zunehmend werden daher Sicherheitsstandards wie die Common Criteria oder anerkannte unabhängige Audit-Standards an Bedeutung gewinnen. Sie fördern das gegenseitige Vertrauen [Rann00].

4 Herausforderungen für das IM

Die eingangs gestellte Frage nach einem schon vorhandenen „Fit“ des IT-Risk Managements für die Herausforderungen des E-Business kann bisher nur bedingt bejaht werden. Wird ITRM als Identifikation, Analyse, Steuerung und Kontrolle der Risiken im Sinne aller Aufgaben des Informationsmanagements verstanden, und erfasst man E-Business neben all seinen Chancen auch als Risk-Driver für das Informationsmanagement, fällt bei der Prüfung der üblicherweise eingesetzten Methoden eine nachhaltige Führungslücke auf. Gerade auf der Modellebene der Informationswirtschaft und der Strategiebildung gibt es wenige Konzepte für ein Risk Management, obwohl die Potenziale des E-Commerce bei der Umsetzung gerade hier einen nachhaltigen Wettbewerbsvorteil verschaffen können. Die Sicherstellung der Funktionsfähigkeit und Verfügbarkeit der Informationstechnologien sowie die Bereitstellung geeigneter Informationssysteme für das E-Business sind lediglich eine notwendige Voraussetzung. Erst hierauf aufbauend können strategisch positionierte Inhalte und Dienstleistungen den erhofften Wettbewerbsvorteil erbringen.

An dieser Stelle wird die Schnittstelle zum unternehmensweiten Risk Management deutlich, gerade bei der Konfiguration von Inhalten ist der Bezug zum Unternehmenskontext unerlässlich. IT-Risk Management muss daher in verstärktem Maße auch in das unternehmensinterne Führungs- und Kontrollsystem integriert werden. Neben dem Management der spezifischen Risiken des IM ist damit eine hinreichende Berücksichtigung der (Rest-)Risiken in der Unternehmensstrategie sichergestellt.

Ein Ansatz für ein effizientes IT-Risk Management wurde in Kapitel 3 mit dem Modell des IT-Risk Managements vorgeschlagen. Die Implementierung eines solchen Prozesses hat gleich mehrere Vorteile. Zum einen handelt es sich nicht um ein statisches Modell sondern stellt durch die Identifikation von situativen Risikoobjekten auch bei sich rasch ändernden Umweltvariablen ein effizientes Instrumentarium sicher. Zum anderen müssen existierende Konzepte, wie sie in Kapitel 2 vorgestellt werden, nicht verworfen werden. Sie sind als Good-Practice Lösungen in Teilbereichen des Risikozyklus, vor allem im Rahmen der Risikoidentifikation, von wesentlicher Bedeutung. Die Berücksichtigung des Integrationsrisikos ermöglicht vor dem Hintergrund des E-Business auch die Berücksichtigung interorganisationaler Interdependenzen.

Gegenstand eines effektiven und effizienten ITRM ist die Verbindung von Geschäftsmodell und Technologie. E-Business Risk ist eine Kombination von Geschäftsmodell (Kundengruppen, Waren, Vertriebsform) und Technologie (Prozesse, Oberfläche, Verfügbarkeit).

Literatur

[Balz98] Balzert, H.: Lehrbuch der Software-Technik: Software-Management, Qualitätssicherung, Unternehmensmodellierung. Spektrum Akademischer Verlag, Heidelberg, Berlin, Oxford 1998.

[Boeh89] Boehm, B. W.: Tutorial: Software Risk Management. IEEE Computer Society Press, Washington 1989.

[Brau84] Braun, H.: Risikomanagement – eine spezifische Controllingaufgabe. Diss., Toeche-Mittler, Darmstadt 1984.

[BuSi99] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzhandbuch – IT-Sicherhheitsmanagement, Bonn, 1999.

[Chor92] Chorafas, D. N.: Globales Risikomanagement. In: Globales Risikomanagement in Finanzinstitutionen. Gabler, Wiesbaden 1992.

[CoCr01] o.V.: Common Criteria for Information Security Evaluation. Part 1: Introduction and general model. In: http://www.commoncriteria.org/docs/PDF/ CCPART1V21.PDF, Abruf am 2001-01-12.

[Farn79] Farny, D.: Grundfragen des Risk Management. In: Risk Management – Strategien zur Risikobeherrschung. Hrsg: Goetzke, W.; Sieben, G.. Gebera-Schriften, Band 5, Gebera, Köln 1979, S. 11-37.

[Fass95] Fasse, F.-W.: Risk-Management im strategischen internationalen Marketing. In: Duisburger Betriebswirtschaftliche Schriften. Diss., Hrsg: Barth, K. et al.. Band 10, S+W Steuer- und Wirtschaftsverlag, Hamburg 1995.

[GlKö99] Gleich, R.; Kögler, S.: Hat Ihr Controlling die Risiken im Griff? – Überlegungen für ein Risikomanagement-System. In: IS-Report. 3. Jg. (1999) Nr. 9, S. 10-15.

[Hein91] Heinen, E.: Industriebetriebslehre – Entscheidungen im Industriebetrieb. 9. Aufl., Gabler, Wiesbaden 1991.

[HoMa98] Hommelhoff, P.; Mattheus, D.: Corporate Governance nach dem KonTraG. In: Die Aktiengesellschaft. 43. Jg. (1998) Nr.6, S. 249-259.

[InSe99] o.V.: Enough is (Never) Enough. In: Information Security Magazine, (1999) Nr. 6, in http://www.infosecuritymag.com/july99/enough.htm, Abruf am 2000-03-23.

[ISAC00] o.V.: COBIT Executive Summary. Hrsg: Information Systems Audit and Control Foundation. 3. Aufl., Rolling Meadows 2000.

[Kend98] Kendall, R.: Risk Management: Unternehmensrisiken erkennen und bewältigen. Gabler, Wiesbaden 1998.

[Klet93] Klett, G.: Risiko-Analyse mit Fuzzy-Logik. In: KES Zeitschrift für Kommunikations- und EDV-Sicherheit. 9. Jg. (1993) Nr. 6, S. 28-32.

[KrBu94] Krcmar, H.; Buresch, A.: IV-Controlling – Ein Rahmenkonzept für die Praxis. In: Controlling. 6. Jg. (1994) Nr. 5, S. 294-304.

[Krcm00] Krcmar, H.: Informationsmanagement. 2. Auflage, Springer, Berlin 2000.

[Lück98] Lück, W.: Internes Überwachungssystem (IÜS) – Die Pflicht zur Errichtung eines Internen Überwachungssystems durch das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG). In: WPK-Mitteilungen. 37. Jg. (1998) Nr. 3, S. 182-188.

[Mach99] Macharzina, K.: Unternehmensführung: Das internationale Managementwissen; Konzepte, Methoden, Praxis. 3. Aufl., Gabler, Wiesbaden 1999.

[Pali01] Paliotta, A. R.: A Personal View of a World Class IT Auditing Function. In: http://www.isaca.org/art11.htm, Abruf am 2001-01-07.

[Rann00] Rannenberg, Kai: Mehrseitige Sicherheit – Schutz für Unternehmen und ihre Partner im Internet, in: Wirtschaftsinformatik, 42. Jg., Nr. 6 (2000), S. 489-497.

[Rock79] Rockart, J. F.: Chief Executives define their own data needs. In: Harvard Business Review. 57. Jg. (1979) Nr. 2, S. 81-93.

[Scho92] Scholl, W.: Informationspathologien. In: Handwörterbuch der Organisation. Hrsg: Frese, E.. 3. Aufl., Poeschel, Stuttgart 1992, Sp. 900-912.

[ScKr94] Schwarzer, B.; Krcmar, H.: Neue Organisationsformen. In: Information Management. 9. Jg. (1994) Nr.4, S. 20-27.

[Stud98] Studer, G.: Risikomanagement – VAR als Risiko. In: Schweizer Bank. 13. Jg. (1998) Nr. 9, S. 54-59.

[Timm98] Timmers, Paul: Business Models for Electronic Markets. In: EM – Electronic Markets, Vol. 8, No. 2, 1998.

[Voßb93] Voßbein, R.: Der Schutz von IT-Systemen: Praktikable Konzepte. In: KES Zeitschrift für Kommunikations- und EDV-Sicherheit. 8. Jg. (1993) Nr. 2, S. 40-48.