# IT-Risikomanagement bei Unternehmens-fusionen

Detlef Hühnlein

secunet Security Networks
Sudetenstr. 16, 96247 Michelau
detlef.huehnlein@secunet.de

### Zusammenfassung

Dieser Beitrag widmet sich dem Management von IT-Risiken bei Unternehmensfusionen. Insbesondere wird ein praktikables IT-Risikomanagement-System und die Einbettung desselben in existierende Änderungs- und Konfigurationsmanagement-Prozesse skizziert.

## 1 Einleitung

Wie beispielsweise der Zusammenschluß von Daimler und Chrysler, Allianz und Dresdner Bank, DG- und GZ-Bank, Compaq und Hewlett Packard oder die jüngste Fusion der Hypothekenbanken von Deutsche Bank, Dresdner Bank und Commerzbank zur Eurohyp AG belegen, sind Unternehmensakquisitionen und -fusionen ein populäres Mittel um strategisch günstige(re) Wettbewerbspositionen zu erreichen. Damit das vielzitierte, einer Unternehmensfusion vermeintlich innewohnende, Synergie-Potenzial ausgeschöpft werden kann, müssen strategische, organisatorische und operative Einheiten zu einer homogenen neuen Unternehmung integriert werden. Dieser Integrationsprozeß bringt häufig einschneidende Veränderungen mit sich, deren Planung und Umsetzung oft mit erheblichen Risiken verbunden ist. Das effiziente Management dieser Risiken ist ein kritischer Faktor für die erfolgreiche Unternehmensfusion.

Insbesondere bei Unternehmen, z.B. im Finanzdienstleistungssektor, deren Produkte keinen stofflichen Charakter haben, sondern vielmehr Informationen sind, die in der Regel elektronisch verarbeitet werden, kommt der Integration der IT-Infrastrukturen, und dem Management der damit verbundenen Risiken, eine besondere Bedeutung zu. Im Hinblick auf eine effiziente Integration der IT-Infrastrukturen, scheint eine systematische Behandlung von IT-Risiken äußerst ratsam. Deshalb wird in diesem Beitrag ein Vorschlag für ein pragmatisches IT-Risikomanagement-System für Unternehmensfusionen skizziert.

Dieser Beitrag ist folgendermaßen gegliedert: Abschnitt 2 skizziert die typischen Phasen einer Unternehmensfusion. In Abschnitt 3 findet sich ein Vorschlag für ein pragmatisches IT-Risikomanagement System, das im Kontext umfassender Veränderungen der IT-Infrastruktur, z.B. im Zusammenhang mit Unternehmensfusionen, eingesetzt werden kann. Abschnitt 4 widmet sich schließlich den größten (Meta-) IT-Risiken bei Unternehmensfusionen.

# 2 Fusionsprozeß

In diesem Abschnitt wird der typische Ablauf eines Fusionsprozesses skizziert. Das Verständnis des hier präsentierten Gesamtablaufes einer Unternehmensfusion ist für die adäquate Einordnung der IT-Risikomanagementaufgaben in den Gesamtprozeß wichtig.

Wie in **[GaHe99]** (Kapitel 1, SS. 8 ff) ausführlicher erläutert, kann eine Unternehmensakquisition oder - fusion in folgende Phasen eingeteilt werden:

- **Strategie**

  In dieser Phase spielen insbesondere strategische Überlegungen, wie die Formulierung einer Geschäftsstrategie oder die Festlegung von Kriterien für Akquisitions- bzw. Fusionsobjekte eine Rolle.

- **Identifikation**

  In dieser Phase wird das Unternehmen ausgewählt, das möglicherweise akquiriert, bzw. mit dem möglicherweise fusioniert, werden soll. Außerdem werden hier potentielle Synergien identifiziert und entsprechende Vertraulichkeitsvereinbarungen zwischen den beteiligten Unternehmen geschlossen sowie ein genereller Fusionsplan entworfen, der den weiteren Ablauf festlegt.

- **Untersuchung**

  Diese Phase ist von ausführlichen, sog. "Due-Diligence"-, Untersuchungen, geprägt. Diese Untersuchungen beleuchten insbesondere

  - Finanzielle und rechtliche Aspekte
  - Aspekte der Unternehmenskultur und Mitarbeiter
  - Geschäftsprozesse
  - IT-Infrastrukturen

  vor dem Hintergrund einer möglichen Zusammenführung der Unternehmen. Die Ergebnisse dieser Phase bilden die Grundlage für die nachfolgend durchgeführten Verhandlungen und, was in diesem Beitrag von zentraler Bedeutung ist, den Startpunkt für das Management von IT-Risiken. Insbesondere wird bereits hier eine erste - natürlich nicht nur IT-Aspekte betrachtende - Risikoanalyse durchgeführt.

- **Verhandlung**

  Hier werden die finanziellen, rechtlichen und strukturellen Rahmenbedingungen der Unternehmensfusion ausgehandelt.

- **Integration**

  In dieser abschließenden Phase werden die Integrationspläne für

  - organisatorischen Strukturen,
  - Geschäftsprozesse und
  - IT-Systeme

  näher detailliert und schließlich umgesetzt.

Wie in Abbildung 1 ersichtlich, laufen diese Phasen typischerweise nicht streng sequentiell, sondern teilweise parallel ab.

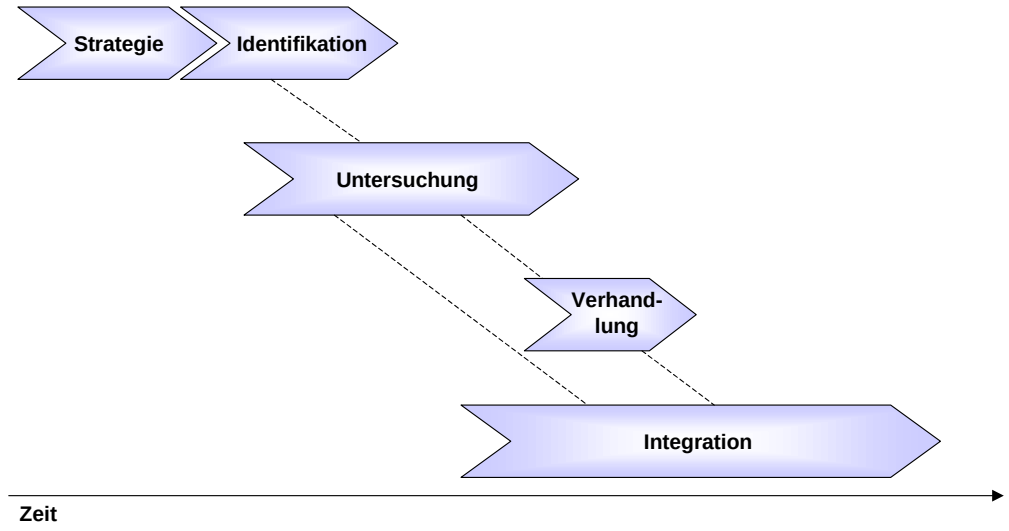


Abbildung 1: Typischer Fusionsprozeß

Das im folgenden Abschnitt vorgeschlagene Verfahren zum Management von IT-Risiken wird in der Untersuchungs- Phase initialisiert und führt während der gesamten Integrationsphase - oder auch darüber hinaus - zu einer systematischen Behandlung von IT-Risiken.

# 3 IT-Risikomanagement bei Unternehmensfusionen

In diesem Abschnitt werden die Grundzüge eines praktikablen Systemes für das Management von IT-Risiken vorgestellt, wie es im Rahmen von Unternehmensfusionen eingesetzt werden kann.

Dieser Abschnitt ist folgendermaßen gegliedert: Abschnitt 3.1 liefert einen kurzen Überblick über die wichtigsten Aspekte des allgemeinen IT-Risikomanagements. In Abschnitt 3.2 wird auf die Einbindung des IT-Risikomanagements in den Fusionsprozeß eingegangen.

## 3.1 Grundlagen des IT-Risikomanagements

In diesem Abschnitt wollen wir die wichtigsten Aspekte des IT-Risikomanagements ins Gedächtnis zurückrufen.

Ziel des *Risikomanagements* ist es, die mit einer bestimmten Unternehmung verbundenen Risiken - durch Vermeidung, Verminderung, Begrenzung oder Übertragung - auf ein tragbares Maß zu reduzieren.

Die Größe eines *Risikos* lässt sich als das Produkt der beiden Faktoren Schadenshöhe und Eintrittswahrscheinlichkeit begreifen.

Liegen für diese beiden Faktoren exakte Werte oder zumindest (zuverlässige) Schätzungen vor, so lässt sich ein Risiko "bepreisen". Somit können Risiken in betriebswirtschaftliche Ü-

berlegungen einfließen. Beispielsweise können so, wie z.B. in **[Bitz00]** erläutert, methodisch unterlegte Entscheidungen unter Risiko und Ungewissheit durchgeführt werden. Außerdem besitzt die Ermittlung und Verwaltung von Risiken in der Finanzdienstleistungsbranche, insbesondere vor dem Hintergrund von Basel II, eine große Bedeutung.

Während bei finanzwirtschaftlichen Risiken, wie Markt- und Kreditrisiken, die Schadenhöhe meist bekannt oder gut abschätzbar ist und deshalb die, in der Subjektivität begründete, Unschärfe in der Risikoermittlung auf das Abschätzen der Wahrscheinlichkeit, und ggf. (bei der Kumulation einzeln ermittelter Risiken zum Gesamtrisiko) der Korrelationsparameter, begrenzt ist, ist bei der Betrachtung von IT- und Betriebsrisiken meist auch die Schadenhöhe kaum zuverlässig abschätzbar. Deshalb ist der Vorschlag in **[Buhr00]**, auch Betriebsrisiken mit dem sonst üblichen Value-at-Risk-Ansatz (siehe z.B. **[OeUn01]**) zu messen, zwar theoretisch ansprechend, aber in der Praxis kaum eingesetzt, da vor dem Hintergrund höherer adminstrativer Aufwände der Mehrwert einer vermeintlich exakteren Risikomessung vergleichsweise gering erscheint.

Wird eine exakte Messung des Betriebsrisikos nicht durch Aufsichtsbehörden, wie z.B. das Bundesaufsichtsamt für das Kreditwesen, gefordert, so begnügt man sich in der Praxis, wie in Abbildung 2 dargestellt, oft mit einer groben Klassifizierung.

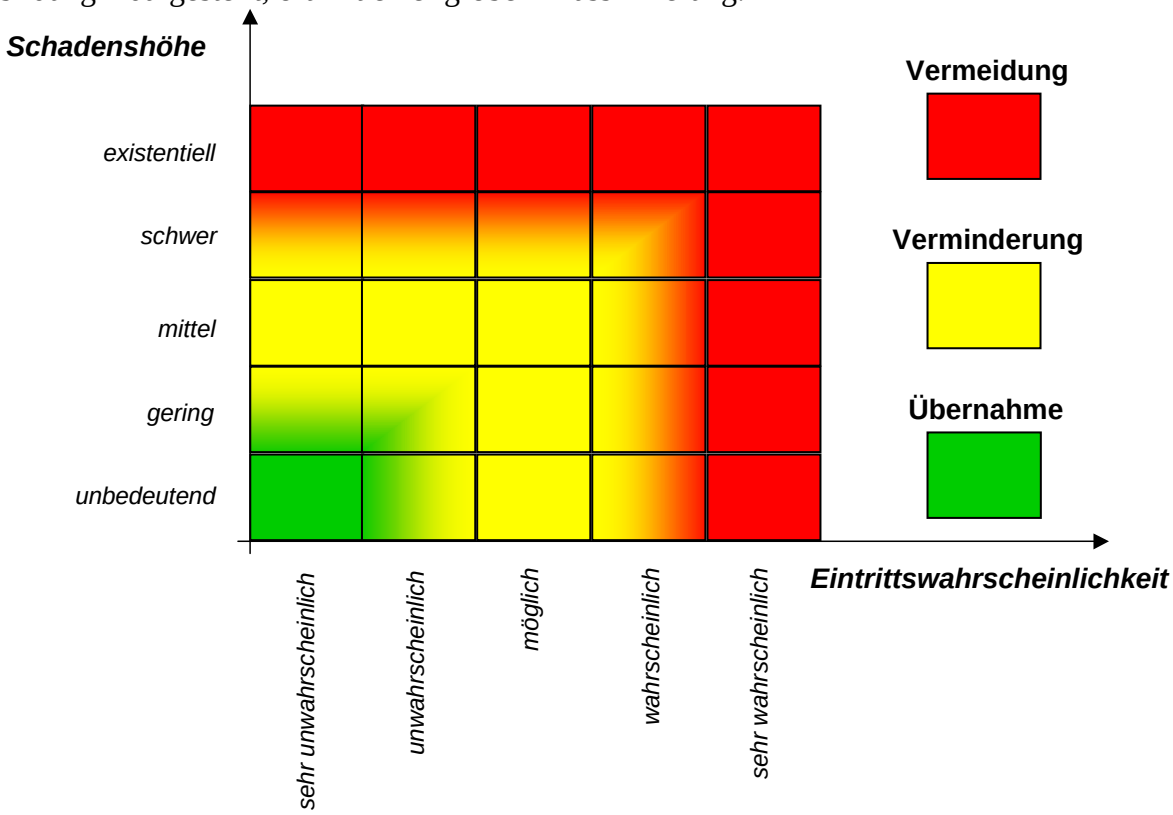


Abbildung 2: Risikomatrix zur Klassifizierung von Risiken

Gemäß dem oben angegebenen Ziel ist das IT-Risikomanagement ein Prozeß, der für alle existierenden Risiken iterativ die folgenden Schritte durchführt, bis idealerweise alle Risiken auf ein tragbares Maß reduziert sind:

- Risikoanalyse
- Festlegung von Maßnahmen zur Verminderung der Risiken
- Detailplanung und Implementierung der Maßnahmen
- Kontrolle der Wirksamkeit der Maßnahmen / erneute Risikoanalyse

Die Maßnahmen zur Verminderung der Risiken zielen also darauf ab, die Eintrittswahrscheinlichkeit eines Schadensfalles und/oder die Schadenhöhe zu minimieren.

Organisatorisch sollte für jedes im Rahmen der Risikoanalyse identifizierte, und gemäß der Risikomatrix eingeordnete, Risiko ein *Risikoeigentümer* festgelegt werden, der für die Ermittlung der Risiken sowie der Planung, Umsetzung und Bewertung der risikovermindernden Maßnahmen verantwortlich ist. Die Risikoeigentümer berichten in regelmäßigen Abständen an einen zentralen *Risikomanager*, der möglicherweise übergeordnete Risiken, wie z.B. zeitliche Verzögerungen in abhängigen Teilprozessen oder Risiken beim Zusammenwirken verschiedener (Risiko-)Komponenten, erkennen kann und zusammenfassende Risikoberichte, über den aktuellen Status und die Veränderungen von Risiken über längere Zeiträume, für das übergeordnete Management erstellen kann.

Diese hier skizzierten Aspekte des IT-Risikomanagements sollten in einer verbindlichen, von der Unternehmensleitung unterstützten, IT-Risk-Policy festgelegt sein, die zumindest die folgenden Punkte umfasst:

**1. Zielsetzung und Anwendungsbereich**

Hier wird die grundlegende Zielsetzung und der Anwendungsbereich der IT-Risk-Policy als Dokument und des IT-Risikomanagements, in organisatorischer und prozeduraler Hinsicht, dargelegt. So könnte das generelle Ziel des Risikomanagements sein, existierende Risiken in "definierter Art und Weise" durch entsprechende Maßnahmen auf ein "tragbares Maß" zu reduzieren.

Welche Rollen für welche Prozesschritte verantwortlich sind, und anhand welcher Kriterien ein Risiko als tragbar bezeichnet wird, wird in weiteren Kapiteln der IT-Risk-Policy geregelt.

Ein weiterer Punkt, der hier Beachtung finden sollte, sind existierende Schnittstellen zu weiteren Policies, wie z.B. der IT-Security-Policy, und deren Ausführungsbestimmungen. So kann es bei der Identifikation und Systematisierung der verschiedenen Risiken vorteilhaft sein, sich der in der IT-Security-Policy definierten Schutzziele

- Integrität
- Vertraulichkeit
- Verbindlichkeit / Authentizität
- Verfügbarkeit

zu bedienen. Denn alle IT-Risiken erwachsen aus Verletzungen dieser vier Schutzziele, wobei die Verfügbarkeit eines Systemes oder Prozesses im Rahmen eines zeitlichen *und*

*monetären* Budgets gemeint ist. Deshalb bedarf es möglicherweise einer ergänzenden Präzisierung der Begriffsbestimmungen.

2. **Rollen und Verantwortlichkeiten**

   Hier werden die in den Risikomanagement-Prozeß eingebundenen Rollen definiert und entsprechende Verantwortlichkeiten zugewiesen.

3. **Klassifizierung von Risiken**

   Da Risiken, abhängig von Ihrem Ausmaß eine unterschiedliche und entsprechend priorisierte Behandlung erfahren sollen, müssen, wie in Abbildung 2 skizziert, verschiedene Klassen eingeführt werden. Die Grenzwerte sollten hierbei idealerweise mit konkreten Werten belegt werden. Ist die Festlegung konkreter Werte (z.B. "sehr wahrscheinlich" meint eine Wahrscheinlichkeit größer als p=0.1, oder "existenzieller Schaden" beginnt ab 5 Millionen €) schwierig, so sollte zumindest die Definition der Schwellwerte durch Beispiele unterlegt werden.

4. **Definition des IT-Risikomanagement-Prozesses**

   Hier wird der grundsätzliche Ablauf des Risikomanagement-Prozesses festgelegt. Ein Beispiel, wie dieser Risikomangement-Prozess, vor dem Hintergrund einer Unternehmensfusion in den Konfigurationsmanagment-Prozess eingebunden werden kann, findet sich in Abschnitt 3.2.

## 3.2 Einbindung des IT-Risikomanagements in den Fusionsprozeß

Da die IT-Infrastrukturen bei Unternehmensakquisitionen oder -fusionen oft tiefgreifenden Veränderungen ausgesetzt sind, deren Umsetzung außergewöhnliche Risiken induziert, wird empfohlen, ergänzend zum operativen Fusionsprozeß einen Prozeß für das Management der mit der Fusion verbundenen IT-Risiken zu etablieren, bzw. diesen - falls entsprechende Prozesse für das IT-Risikomanagement bereits existieren - mit dem Fusionsprozeß zu harmonisieren.

Die entsprechenden Regularien sollten im Rahmen der neu zu erstellenden, bzw. anzupassenden, IT-Risk-Policy formuliert werden. Außerdem sollten weitere bestehende Regularien, wie z.B. die IT-Security-Policies der fusionierenden Unternehmen, harmonisiert und möglicherweise um entsprechende Übergangsregelungen ergänzt werden.

Im Folgenden wird skizziert, wie das IT-Risikomanagement elegant in den gesamten Fusionsund Integrationsprozeß eingebunden werden kann.

Wir gehen davon aus, dass der operative Integrationsprozeß der IT-Infrastrukturen bei einer Fusion durch ein - oftmals bereits existierendes - Änderungs- und Konfigurationsmanagement-System unterstützt wird. Dieses Konfigurationsmanagement-System berücksichtigt die folgenden Prozeßschritte:

- Produktivbetrieb
- Änderungsantrag
- Detailplanung der Änderungen

- Implementierung der Änderungen in Testumgebung
- Qualitätssicherung
- Übernahme der Änderungen in den Produktivbetrieb

Um die durch die Fusion von IT-Infrastrukturen induzierten Risiken effizient handhaben zu können, wird empfohlen den Riskikomanagement-Prozeß - wie in Abbildung 3 dargestellt - in die existierenden Änderungs- und Konfigurationsmanagement- Prozesse zu integrieren.

Hierbei wird für jede - von der Integrationsplanung initiierte - Änderung der jeweilige Risi-

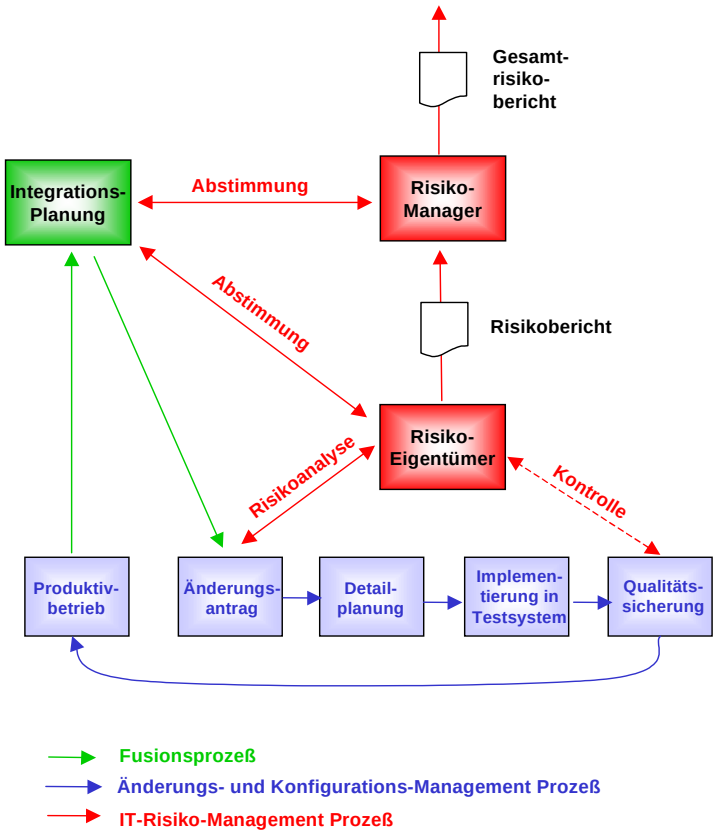


Abbildung 3: Integration des IT-Risikomanagements in Änderungs- und Konfigurationsmanagement

koeigentümer, z.B. der betroffene Teilprojektleiter, mit der Durchführung einer Risikoanalyse für die geplante Änderung beauftragt. Nach der Implementierung in einer Testumgebung wird eine erneute Risikoanalyse durchgeführt und der Status, sowie etwaige Abweichungen in einem Risikobericht an den Risikomanager geschickt. Der Risikomanager führt die einzelnen Risikoberichte zu einem Gesamtrisikobericht für übergeordnete Organisationseinheiten, d.h. unter Umständen die Unternehmensleitung, zusammen. Muss durch aufsichtsrechtliche Bestimmungen, z.B. durch Basel II im Kreditgewerbe, das Gesamtrisiko exakt bemessen werden, damit entsprechendes Eigenkapital hinterlegt werden kann, so muss der Risikomanager die Korrelationsparameter zur Aggregierung der Einzelrisiken zum Gesamtrisiko ermitteln oder, ggf. unter Rücksprache mit den einzelnen Risiko-Eigentümern, abschätzen.

Werden bei der Erstellung oder Überprüfung der Risikoberichte Risiken offenbar, die nicht getragen werden sollen, so kann sich der betreffende Risikoeigentümer oder der Risikomana-

ger mit der Integrationsplanung abstimmen um weitere Änderungen zu initiieren, die auf die Reduktion der Risiken abzielen.

Diese Prozesse sind wiederum in organisationsübliche Revisionsprozesse einzubinden. Dies ist wichtig, da sich, wie in **[Brin01]** erläutert, das - u.a. durch die Arbeit der unabhängigen Innenrevision implementierte - Vier-Augen-Prinzip als sehr wichtiges Risikomanagement-Werkzeug begreifen lässt.

Der Beginn dieses (IT-) Risikomanagement-Prozesses besteht aus der erstmaligen Identifikation der mit der Fusion verbundenen (IT-) Risiken, die in der in Abbildung 1 dargestellten Untersuchungsphase durchgeführt werden sollte.

# 4 Besondere IT-Risiken bei Unternehmensfusionen

In diesem Abschnitt werden einige zusätzliche IT-Risiken bei der Unternehmensfusion aufgelistet und entsprechende Maßnahmen zur Verminderung dieser Risiken angedeutet.

Wie in Abschnitt 3.1 erläutert, haben alle IT-Risiken Ursachen in der Verletzung der allgemeinen Sicherheits-Ziele (Integrität, Vertraulichkeit, Verbindlichkeit und Verfügbarkeit). Deshalb verzichten wir hier bewusst auf eine ausführliche Behandlung der allgemeinen Betriebsrisiken, die mit Informationssystemen zusammenhängen, und deren sicherheitsrelevanten Ursachen und verweisen statt dessen auf **[Brin01]** und **[BSI01]**.

Wir greifen hier lediglich einige Meta-Aspekte auf, die bei Unternehmensfusionen zu *zusätzlichen* IT-Risiken führen können und dementsprechend zu beachten sind:

- Change-Management-System als zentrale Komponente des Fusionsprozesses

  Ein ungeordneter Change-Managment-Prozeß gehört zu den wichtigsten Quellen für weitere IT-Risiken, die sich im Verlust der Integrität, Vertraulichkeit, Verbindlichkeit und vor allem Verfügbarkeit diverser IT-Systeme ausdrücken können.

  Hier wird empfohlen den existierenden Change-Management-Prozeß auf seine Leistungsfähigkeit hin zu überprüfen und ggf. zu ergänzen. Im Rahmen dieser Überprüfung sollten auch Aspekte des IT-Risikomanagements, wie in Abschnitt 3.2 erläutert, in den Konfigurations-Management-Prozess integriert werden.

- Inkompatibilität normativer Elemente

  Während im "laufenden Betrieb" einer Organisation normative Elemente, wie Organisationsstruktur sowie Rechte und Pflichten der verschiedenen Entitäten geregelt sind, so sind diese bei fusionierenden Unternehmen meist nicht identisch und oft nicht ohne weiteres kompatibel.

  So ist die Harmonisierung der Organisationseinheiten, Regularien und Kernprozesse eine unabdingbare Voraussetzung für einen erfolgreichen Integrationsprozeß.

  Hier wird empfohlen neben der harmonisierten Organisationsstruktur auch die relevanten Leitlinien zu harmonisieren und ggf. um entsprechende Übergangsregelungen zu ergänzen. Diese Harmonisierung der bestehenden Regularien sollte auch im Rahmen der allgemeinen Change-Management-Abläufe stattfinden und demnach einer Risiko-Analyse unterzogen werden.

- Inkompatibilität von IT-Systemen

Zu den größten Herausforderung auf dem Weg zur Harmonsierung von IT-Infrastrukturen während einer Unternehmensfusion gehört die Lösung von Interoperabilitätsproblemen beim zusammenwirken der eingesetzten IT-Systeme. Das Meta-Risiko in diesem Zusammenhang ist, dass die geplanten Änderungen nicht, oder nicht verhältnismäßigem Aufwand, durchgeführt werden können. Erwartete Synergiepotentiale erweisen sich als nicht ausschöpfbar. Bei Unternehmen mit starker Abhängigkeit von IT-Systemen, kann dies den gesamten Fusionserfolg gefährden.

Deshalb sollten in der Untersuchungsphase auch die Aspekte der Interoperabilität der verschiedenen für eine Harmonisierung vorgesehenen Systeme eingehend untersucht werden. Hierzu scheint es ratsam, sich bei besonders wichtigen IT-Systemen, z.B. für die allgemeinen Kommunikationsmedien (Telefon, Mail, ...), nicht auf Herstelleraussagen zu verlassen, sondern eigene Tests durchzuführen.

- Inkompatibilität von Anwendungen

  Neben der technischen Interoperabilität, stehen einer Harmonisierung häufig auch semantische, anwendungsbezogene, Inkompatibilitäten im Weg. Dies betrifft nicht nur Anwendungen für externe Geschäftsprozesse, sondern auch interne, administrative Anwendungen. Besonders kritisch ist in diesem Zusammenhang die Inkompatibilität von Systemen zur Unternehmenssteuerung. Wie in **[Jopp01]** angedeutet, scheitern viele Unternehmensfusionen schlicht daran, dass sie - aufgrund inkompatibler Controlling-Systeme - "im Blindflug" durchgeführt werden (müssen?).

  Der in **[Jopp01]** vorgeschlagene Ausweg zur Vermeidung dieses Blindfluges ist die Etablierung eines übergeordneten Systemes: "Um den alten Controlling-Systemen keine Konkurrenz zu machen, wählt man dafür meist ein System der analytischen Unternehmenssteuerung oder des Risk-Managements." Somit ist die Bedeutung des Risiko-Managements in der Unternehmensfusion natürlich nicht auf IT-spezifische Belange beschränkt, sondern kann vielmehr (in angepasster Form) auch auf Ebene des Gesamtunternehmens angewandt werden.

# Literatur

**[Bitz00]** M. Bitz: *"Finanz- und risikotheoretische Grundlagen der Betriebswirtschaftslehre"*, Dateikurs, Version 2.1 FernUni Hagen, 2000

**[Brin01]** G. J. van den Brink: *"Operational Risk - Wie Banken das Betriebsrisiko beherrschen"*, Schäfer-Poeschel, ISBN 3-7910-1756-X, 2001

**[BSI01]** BSI - Bundesamt für Sicherheit in der Informationstechnik: *"IT-Grundschutzhandbuch"*, Version 2001, via http://www.bsi.de/gshb/deutsch/menue.htm

**[Buhr00]** R. Buhr: *"Messung von Betriebsrisiken: Ein methodischer Ansatz"*, Die Bank, SS. 202-206, 2000

**[GaHe99]** T.J. Galpin, M. Herndon: *"The complete guide to mergers and acquisitions"*, Jossey-Bass Publishers, ISBN 0-7879-4786-5, 1999

**[Jopp01]** J. Joppe: *"Oft bremsen Controlling-Systeme Fusionspläne aus"*, Handelsbatt vom 18.11.2001

**[OeUn01]** A. Oehler, M. Unser: *"Finanzwirtschaftliches Risikomanagement"*, Springer, ISBN 3-54067766-6, 2001