Diplomarbeit im Fach Informatik

Zum Thema:

„Integration von finanziellem und operativem IT Controlling mit dem IT-Risikomanagement: Konzepte und praktische Umsetzung“

Angefertigt am
Institut für Informatik

Universität Zürich
Prof. A. Bernstein

Betreuer:

Ernst & Young
Herr Jürg Brun

Vorgelegt von:

Daniel M. Schmid
7. April 1969
von Zürich
Rankstr. 17
8032 Zürich
schmid.dani@gmx.net

Matrikelnummer 99-708-976

Abgabedatum:

6. Oktober 2003

„Ein Computer arbeitet deshalb so schnell, weil er nicht denkt.“[1]

Für Ilka

[1] Gabriel Laub, Tschechischer Schriftsteller, 1928-1989

Inhaltsverzeichnis

1 Executive Summary

1.1 Deutsch

Wettbewerbsvorteile kann eine Unternehmung heute mehr im reibungslosen Betrieb ihrer IT erlangen, als im Einsatz von ausgefallenen Lösungen. Das Controlling der IT sowie genaue Kenntnisse der von ihr ausgehenden Risiken (Chancen und Gefahren) bilden demnach eine wichtige Kompetenz im Umgang mit Informationssystemen. Eine Integration von IT-Controlling und IT-Risikomanagement bietet Potential für eine effizientere Steuerung von IT und damit Potential für Wettbewerbsvorteile.
Die vorliegende Arbeit hat die Fragen geklärt, ob ein Framework besteht, welches sich mit der Integration von IT-Controlling und IT-Risikomanagement befasst, ob dieses Konzept in der Praxis angewandt wird und wo allenfalls Probleme bestehen. Aufgrund von Literaturarbeit und einer Umfrage in sechs Unternehmungen konnte festgestellt werden, dass kein entsprechendes vollständiges Framework besteht und Teilkonzepte nur partiell zum Einsatz kommen. Die Probleme liegen bei den Schnittstellen, den heterogenen Applikationen sowie dem verfügbaren Datenmaterial.

Im Sinne einer Verbesserung dieser Situation wurde ein Integrationsmodell erarbeitet, welches den oben genannten Problemen möglichst gut entgegentritt. Dazu wurden Anforderungen für ein Integrationsmodell aufgestellt und aufgrund dieser eine geeignete Basis für das zu erstellende Modell bestimmt. Als Basis kamen CobIT, ITIL, ARIS, ISO17799 sowie XBRL[2] in Frage. Am besten abgeschnitten hat dabei der technische Standard XBRL. Das entwickelte Integrationsmodell, in der Arbeit ‚Extended_XBRL' genannt, basiert daher auf den Ideen von XBRL. ‚Extended_XBRL' versucht IT-Controlling und IT-Risikomanagement anhand eines geeigneten Datenmodells integriert abzubilden. Neben technischen Faktoren werden auch nicht-technische Rahmenbedingungen einbezogen. Zur Verifizierung des vorgeschlagenen Integrationsmodells wurde eine Fallstudie anhand realer Daten durchgespielt. Diese qualifizierte den Ansatz von ‚Extended_XBRL' als tauglich.

[2] XBRL ist Akronym für 'Extended Business Reporting Language'

Umsetzungsorientiert wurden Handlungsempfehlungen formuliert und eine Quick Reference mit den wichtigsten Erkenntnissen zusammengestellt. Diese Quick Reference steht als eigenständiges Dokument zur Verfügung.

1.2 English

Nowadays, a company achieves competition advantages more by running a smooth IT than using extraordinary solutions. Controlling of its IT and knowledge of IT inherent risks (chances and dangers) are therefore an important capability in handling information systems. An integration of IT-Controlling and IT-Risikomanagement offers potential for a more efficient control over IT and thus, potential for competition advantages.

The presented work clarified the questions whether a Framework exists, which describes an integration of IT-Controlling and IT-Risikomanagement, whether this concept is used in practice and where possible problems are located. Literature work and an inquiry in six enterprises stated that no appropriate, complete Framework exists and that incomplete concepts are used only in part. Most problems arise with data interfaces, heterogeneous applications and with the availability of data.

In the sense of an improvement of this situation, an integration model was developed which faces the mentioned problems as well as possible. To do so, requirements were set up for an integration model. Based on the found requirements, a suitable base for the integration model was defined. Under consideration were CobIT, ITIL, ARIS, ISO17799 as well as XBRL[3]. The most excellent base provided the technical standard XBRL. The proposed integration model, built in this work is declared as 'Extended_XBRL '. It is based on the ideas of XBRL. 'Extended_XBRL' tries to model IT-Controlling and IT-Riskmanagement in a suitable integrated way. Apart from technical factors, non-technical environmental conditions were also included. A case study with real data was used to verify the suggested integration model. This qualified the approaches followed by Extended_XBRL as suitable.

[3] XBRL is stands for 'Extended Business Reporting Language'

Recommendations for business action were formulated and a Quick Reference with the most important facts about integration of IT-Controlling an IT-Riskmanagement was created. This Quick Reference is available as an independent document.

2 Einleitung

2.1 Bezug

In den vergangenen Jahren und Jahrzehnten war die IT stark Technologie getrieben. Das Neuste, das noch bessere musste in kürzester Zeit implementiert werden. Das Blatt scheint sich langsam zu wenden, von einer technologischen Sicht der IT zu einer ökonomischen Sicht[4]. Dabei sind Begriffe wie Effektivität und Effizienz zentral.

Unter dem provokanten Titel "IT Doesn't Matter"[5] kommt Nicholas G. Carr in seinem Artikel in der Harvard Business Review zu dem Ergebnis, dass Unternehmen durch Investitionen in Informationstechnologie heute keine strategischen Wettbewerbsvorteile mehr erzielen, sich also dadurch nicht dauerhaft von ihren Mitbewerbern abheben können. Zunächst einmal ist IT für Carr eine Infrastrukturtechnologie wie Elektrizität oder die Eisenbahn. Wie die Entwicklung dieser Technologien zeigt, konnte ein Unternehmen zwar in der Phase der Einführung durch schnelle und intelligente Nutzung die eigene Marktposition verbessern, nachdem sich die Technologie etabliert hatte aber nicht mehr. Allerdings sind Elektrizität wie auch IT mittlerweile für Unternehmen essenziell, so dass ein Funktionsausfall dieser Infrastruktur dramatische Konsequenzen hat. Deshalb fordert Carr, dass Unternehmen stärker die potenziellen Verwundbarkeiten des Unternehmens durch (nicht funktionierende) IT im Auge behalten sollten. Damit gemeint ist das IT-Risikomanagement.

Dem anzufügen ist, dass heute Wettbewerbsvorteile mittels dem von Carr angesprochenem IT-Risikomanagement auch durch den Ausbau eines Instrumentariums zur effektiven und effizienten Steuerung der IT erzielt werden können.

[4] [STRASSMANN90]
[5] [Carr03]

Gemäss den Aussagen von Carr soll sich die IT auf die effiziente und sichere Erledigung ihrer Aufgaben beschränken, genau wie das Elektrizitätslieferanten tun[6]. Genau damit befasst sich die vorliegende Arbeit. Es geht hier nicht primär um die Vorstellung einer neuen Technologie oder eines neuartigen Konzeptes, sondern vielmehr um den effektiven und effizienten Einsatz der IT sowie Chancen und Risiken welche von ihr ausgehen. Klassisch beschäftigt sich das Controlling mit der Sicherstellung von Effektivität und Effizienz. Das IT-Risikomanagement befasst sich mit Gefahren, welche von der IT ausgehen. Die vorliegende Arbeit ist den Bereichen IT-Controlling und IT-Risikomanagement zuzuordnen.

2.2 Situation

Risikomanagement beschäftigt sich mit der quantitativen Abschätzung von Planabweichungen in der Zukunft. Dazu müssen im einfachsten Fall 2 Faktoren bestimmt werden. Die Auswirkungen eines Ereignisses bei Eintreten und die Eintretenswahrscheinlichkeit.

Risiko = Auswirkungen eines Ereignisses bei Eintreten x Eintretenswahrscheinlichkeit

Risiken bilden eine wichtige Entscheidungsgrundlage für die Unternehmensführung. Es ist daher erstrebenswert, das Risikomanagement zu optimieren. Die hier vorliegende Arbeit befassen sich genau damit. Es wird untersucht, wie Informationen aus dem IT-Controlling (finanziell/operativ) für das Risikomanagement in einer integrierten Umgebung verwendet werden können und wo dabei Probleme bestehen.

Die vorliegende Arbeit hat weder IT-Controlling noch Risikomanagement zum Hauptthema. Vielmehr interessieren die Verbindungen zwischen den beiden Gebieten und die damit verbundenen Schwierigkeiten.

Die Integration von IT-Controlling und IT-Risikomanagement wird einerseits formal, anderseits empirisch untersucht. Formal wird untersucht, ob bereits ein Framework für einen integrativen Ansatz besteht und wenn nicht, wie ein solcher Ansatz aussehen könnte. Empirisch wird untersucht, ob integrative Ansätze in der Praxis

[6] In manchen Fällen ist das nicht der Fall, wie die jüngere Geschichte der US Elektrizitätsindustrie gezeigt hat. Analoge Szenarien sind künftig auch bei der IT denkbar.

eingesetzt werden und wo dabei die Probleme liegen. Zur Beantwortung dieser Fragen wurden die unter 2.4 folgende Hypothese aufgestellt. Doch zuvor sollen einige Begriffe geklärt werden.

2.3 Begriffsdefinitionen

2.3.1 Risikomanagement

Die Definitionen von Risiko reichen von 'Gefahr einer Fehlabweichung' bis zur mathematischen Definition 'Risiko = Wahrscheinlichkeit x Impact. Eine häufige Definition betrachtet Risiken als die Möglichkeit eines Schadens oder Verlustes als Konsequenz eines bestimmten Verhaltens oder Geschehens; dies bezieht sich auf Gefahrensituationen, in denen nachteilige Folgen eintreten können, aber nicht müssen. Weniger häufig werden Risiken in Chancen und Gefahren aufgeteilt, je nach dem ob das unsichere Ereignis positive oder negative Folgen hat.

Risikomanagement

Risikomanagement, das auch als Risk-Management oder Risikopolitik bezeichnet wird, ist eine Form der Unternehmensführung, welche auf die Reduktion von Risiken abzielt. Risiken werden in diesem Zusammenhang als Informationsdefizite über das Erreichen von Zielen verstanden. Risikomanagement vollzieht sich in verschiedenen Phasen. Im Anschluss an die Risikoidentifikation folgt die Risikoanalyse, die eine Untersuchung und Bewertung des jeweils vorliegenden Ursache-Wirkungs-Komplexes umfasst. Schließlich werden in Form von Risikovermeidung, Risikominderung, Risikoteilung, Schadenverhütung, Risikoreservebildung sowie Schadenkostenüberwälzung risikopolitische Massnahmen ergriffen.

2.3.2 Controlling

Controlling ist ein Instrument zur Führung eines Unternehmens. Der Begriff geht zurück auf das englische to control ("steuern“, "lenken"). Neben der Steuerung sind Planung und Kontrolle die Hauptaufgaben des Controlling. Das Controlling stellt den Führungskräften Informationen zur Verfügung; damit sollen Probleme frühzeitig erkannt und somit schon im Ansatz umgangen werden. Das Controlling ist ein Subsystem der Führung und umfasst die Gesamtheit aller Institutionen, Prozesse und

Instrumente, mit denen Planung und Kontrolle der Aktivitäten der Unternehmensbereiche koordiniert werden.7

2.3.3 IT-Controlling

Das IT-Controlling befasst sich mit dem Controlling der Informationsinfrastruktur, ist also wiederum ein Teilsystem des Unternehmenscontrollings. Nicht mit dem IT-Controlling zu verwechseln ist die Informatikunterstützung des Controllings durch Tools.

2.3.4 Integration

Eher technologielastig könnte Integration definiert werden als “die Fähigkeit verschiedener Computersysteme zusammenzuarbeiten”. Nicht auf technische Systeme bezogen, befasst sich Integration mit der Fähigkeit von Organisationen zusammenzuarbeiten. Dabei sind Menschen, Technologien und Organisationsstrukturen betroffen.

2.4 Hypothese

In der vorliegenden Arbeit wird die unten stehende Hypothese bearbeitet. Was das genau bedeutet und wie dies erreicht werden soll, wird in den folgenden Kapiteln genauer erläutert.

„(a) Für die Integration von finanziellem und operativem IT Controlling mit dem Risikomanagement besteht ein geeignetes Framework. (b) Das Framework wird in der Praxis jedoch nicht angewandt. (c) Die Probleme bei der Umsetzung liegen hauptsächlich bei den Schnittstellen zwischen den Bereichen, den heterogenen Applikationen sowie dem vorhandenen Datenmaterial.“

2.5 Ziele der Arbeit

Die Ziele der Arbeit gliedern sich in die Bereiche Hypothese sowie zu erstellendes Integrationsmodell.

2.5.1 Betreffend Hypothese

Die vorliegende Arbeit hat zum Ziel, die gestellte Hypothese zu falsifizieren oder zu verifizieren.

[7] in Anlegnung an [LEGAMEDIA]

Wenn ein geeignetes Framework existiert, wird dieses ausführlich beschrieben, sowie dessen praktische Umsetzung genauer untersucht. Der praktische Einsatz eines bestehenden Framework wird empirisch belegt.
Wenn kein geeignetes Framework existiert, werden existierende Teile ausführlich beschrieben, sowie dessen praktische Teilumsetzung genauer untersucht.
Ein spezielles Augenmerk wird auf spezifische Schnittstellenprobleme, heterogene Aplikationen sowie die Verfügbarkeit von geeignetem Datenmaterial gerichtet.

2.5.2 Betreffend Integrationsmodell

Aus den gewonnenen Erkenntnissen werden ein geeignetes Integrationsmodell sowie Handlungsempfehlungen für den praktischen Einsatz formuliert. In Form einer Quick Reference wird das Wissen potentiellen Anwendern verfügbar gemacht.

2.6 Vorgehensweise

Im theoretischen Abschnitt 3 (Konzepte) werden bestehende Konzepte genauer beschrieben. Dabei wird der erste Teil der Hypothese bearbeitet. Es soll (a) festgestellt werden, ob das erwähnte Framework besteht.

Im praktischen Abschnitt 4 (Interviews) wird empirisch festgestellt, ob (b) ein allenfalls vorhandenes Framework umgesetzt wird und wenn nicht, wo die Ursachen dafür liegen. Weiter wird (c) untersucht, ob die Probleme bei der Umsetzung hauptsächlich bei den Schnittstellen, heterogenen Tools sowie dem Datenmaterial zu suchen sind.

Nach den eher analytisch ausgerichteten Abschnitten 3 und 4 versucht Abschnitt 5 (Ausgestaltung eines Integrationskonzeptes) konkret ein Integrationsmodell zu erstellen. Dieses Modell wird in Abschnitt 6 (Anwendung in einer Fallstudie) auf seine praktische Tauglichkeit hin überprüft. Abschnitt 7 (Resultate) trägt die Resultate in Kurzform nochmals zusammen und formuliert Schlussfolgerungen in Form von Handlungsempfehlungen. Abschnitt 8 (Schlussbemerkungen & Ausblick) resümiert die Resultate kurz. Der letzte Teil 9 (Quick Reference) stellt die wichtigsten Aspekte nochmals in kürzester Form dar. Die Anhänge sind in einen öffentlichen Anhang sowie einen Anhang mit Sperrvermerk aufgeteilt. CD's mit Code und Interviewaufzeichnungen sind integraler Bestandteil der vorliegenden Arbeit.

3 Konzepte

Risikomanagement soll keine weitere Insel von Führungstools sein. Vielmehr hängt das Risikomanagement in Teilbereichen direkt mit dem Controlling zusammen. Das Controlling liefert einen wichtigen Teil des Inputs für das Risikomanagement. So liefert zum Beispiel das Controlling aus Projekten Daten, welche direkt ins Risikomanagement der BU[8] oder der Unternehmung übernommen werden können. Oft werden die Daten aber gar nicht oder unrichtig übernommen. Doppelerfassungen sind keine Seltenheit. Zur Klarstellung, welche Daten verschoben werden könnten, soll in 3.1 und 3.2 das Wesen eines Risikomanagements sowie eines IT-Controllings gezeigt werden. Erst wenn klar ist, was diese für Aufgaben erfüllen, kann auch diskutiert werden, wie damit verbundene Probleme gelöst werden können.

3.1 Risikomanagement[9]

3.1.1 Risikoklassen

Risiken fallen in den verschiedensten Bereichen an. Die unten in Abbildung 1 dargestellten Risikoklassen stellen nur eine mögliche Klassifizierung dar. Die in der vorliegenden Arbeit betrachteten Risiken bewegen sich schwergewichtig im Bereich der Unternehmensrisiken. Dabei geht es z.B. um Betriebsrisiken der IT oder um IT-Projektrisiken.

Abbildung 1: Risikoklassen

[8] Akronym für 'Business Unit'
[9] [UBSOUTLOOK01]

3.1.2 Risiken sind Chancen & Gefahren

Einfache Basis

Risikomanagement in seiner einfachsten Sichtweise basiert auf einer einfachen Formel:

$$R(E) = p(E) \cdot I(E)$$

Formel 1: einfache Risikoformel

R : Risiko E

p(E) : Eintretenswahrscheinlichkeit von E

I : Auswirkungen, Impact bei Eintreten von E

E : ein beliebiges Ereignis

Hat ein Ereignis unerwünschte Auswirkungen, so spricht man von einer *Gefahr*. Hat ein Ereignis erwünschte Auswirkungen, so spricht man von *Chance*. Sowohl Gefahren als auch Chancen lassen sich Idealerweise monetär ausdrücken. Die daraus resultierenden Risiken münden entweder in einer positiven oder negativen finanziellen Erwartung. Diese werden in der Literatur auch als *Upsiderisk* und *Downsiderisk* bezeichnet.

Dominanz des Downsiderisks

Der Begriff *Risiko* ist intuitiv für die meisten Personen negativ besetzt. Der Terminus Risikomanagement verleitet daher meistens zu einer rein negativen Interpretation. Ein Risikomanagement das sich nur auf die Gefahren ausrichtet, geht aber am Ziel eines effektiven Risikomanagements zumindest teilweise vorbei. Um dem entgegen zu wirken wird in der Praxis das Risikomanagement oft in ein ‚Gefahrenmanagement' und ein ‚Oportunitymanagement' aufgeteilt. Das Gefahrenmanagement wird dabei eigenständig in einer Risikoabteilung (z.B. vom CSO [10]) gemacht. Das Oportunitymanagement liegt meistens in der Verantwortung der BU's[11].

3.1.3 Interdependez von Chance und Gefahr

Gefahren sind unerwünscht und sollen gemieden werden, Chancen möchte man so viele wie möglich haben. Leider sind Gefahren und Chancen meist innig miteinander

[10] Akronym für 'Chief Security Officer'
[11] Business Unit

verbunden. Eine Chance kommt selten ohne damit verbunden Gefahren. Die einfache Betrachtung anhand Formel 1 ist daher zu einfach. Vielmehr hat ein Ereignis sowohl damit verbundene Chancen als auch Gefahren. Erst die aggregierte Betrachtung der Chancen und Gefahren führt zu einer sinnvollen Entscheidung.

Beeinflussung von Ereignissen

Das Eintreten von Ereignissen lässt sich über geeignete Massnahmen mehr oder weniger steuern. Ob es nun besser ist, dass ein Ereignis X eintreten soll oder nicht, hängt davon ab, ob die daraus resultierenden, erwarteten aggregierten Chancen grösser sind als die erwarteten aggregierten Gefahren. Das Chancenpotential soll grösser sein als das Gefahrenpotential. Soll die Verfügbarkeit einer Applikation erhöht werden, so sollen die damit verbundenen Chancen (z.B. weniger unproduktive Zeiten der Mitarbeiter) grösser sein, als die damit verbundenen Gefahren (z.B. Kostensteigerungen).

Entkoppelung von Downsiderisk und Upsiderisk

Bestehen Interdependenzen zwischen Gefahren und Chancen, gehen diese bei einer getrennten Betrachtung von Chancen und Gefahren verloren. Ein umfassendes, effektives Risikomanagement ist so nur eingeschränkt möglich. Für die Ausgestaltung eines Konzeptes zur Integration von IT-Controlling und IT-Risikomanagement soll dieses Potential gewahrt bleiben, ohne aber den Zwang, Risikomanagement wirklich in diesem umfassenden Sinne zu betreiben. Schliesslich soll das Integrationskonzept keine neuen Prozesse vorschreiben, sondern die praktischen Distanzen zwischen IT-Controlling und Risikomanagement verringern helfen.

3.1.4 Risikoverbunde

Die oben in 3.1.3 diskutierte Interdependenz von Chance und Gefahr ist bereits auch ein Risikoverbund, auch wenn es sich um Auswirkungen des gleichen zugrundeliegenden Ereignisses handelt. Im vorliegenden Kapitel soll aber der Verbund von Risiken von verschieden Ereignissen diskutiert werden.

Die Ereignisse ‚Einführung eines neuen Mailsystems' und ‚Einführung eines CRM Systems' erscheinen auf den ersten Blick als unabhängig voneinander. Bei einer Risikoanalyse könnte aber festgestellt werden, dass aufgrund der gleichzeitigen Einführung Ressourcenengpässe entstehen. Dieses Risiko ist nur nach einer Analyse

von Interdependenzen feststellbar und die Quantifizierung gelingt nur bei einer integrierten Betrachtung beider Projekte. Das später vorgestellte Integrationskonzept soll auch hier Abhilfe schaffen.

3.1.5 Risikobereitschaft und Risikofähigkeit[12]

Welche Risiken sollen eingegangen werden?

Erfolgreiche Unternehmen verstehen es besonders gut, nur solche Risiken einzugehen, bei welchen die Chancen erheblich über den Gefahren liegen (vgl. Abbildung 2). Das Upsiderisk muss grösser sein als die damit verbundenen Downsiderisks. Des weiteren wird bei gleichem Erwartungswert immer diejenige Handlungsalternative gewählt mit der geringeren Unsicherheit, auch wenn die Risken tragbar wären.
Ist erst einmal klar, welche Ereignisse wünschenswert sind, daher die damit verbundenen Chancen grösser sind als die Gefahren, hat man sich bereit erklärt, die Gefahren zu tragen und die damit verbundenen Chancen nutzen zu wollen. Die *Risikobereitschaft* ist damit festgelegt. Wie hoch die Risikobereitschaft ist, hängt einerseits ab vom Ausmass der Risikoaversion und anderseits von der Fähigkeit das Risiko auch tragen zu können. Auf die *Risikofähigkeit* soll im folgenden Abschnitt eingegangen werden.

[12] [UBSOUTLOOK01]

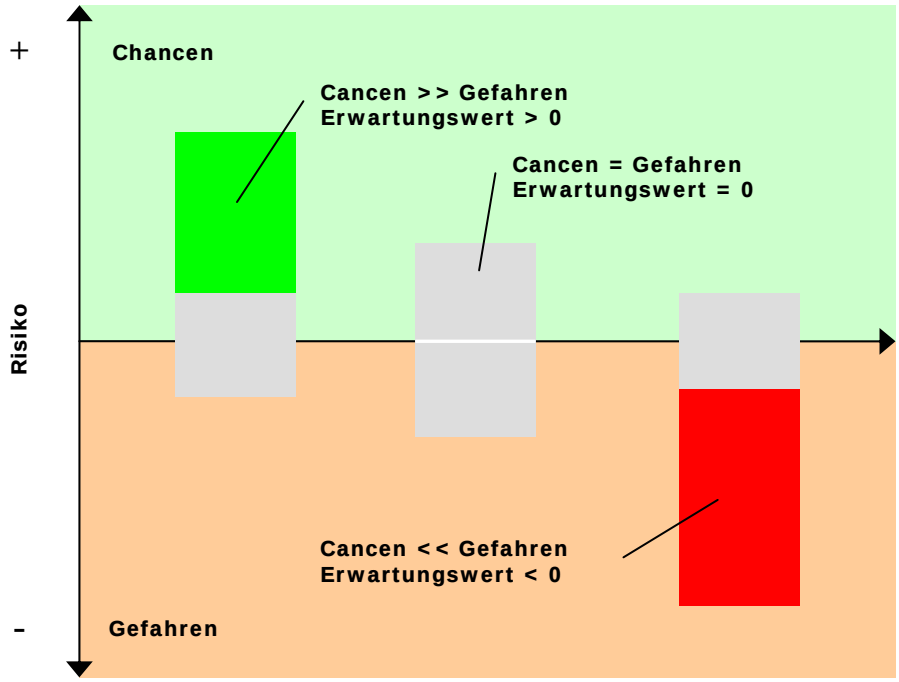

Abbildung 2: Maximierung des Erwartungswertes

Wie viele Risiken kann eine Unternehmung eingehen?[13]

Die Gefahren, denen man sich ausgesetzt hat, müssen möglichst schadlos tragbar sein, d.h. z.B. die Weiterexistenz der Unternehmung ist nicht gefährdet (siehe hierzu 3.1.12). Je nach Grösse und Kapitalkraft der Organisation ist das tragbare Downsiderisk grösser oder kleiner. Tragbare Risiken bemessen sich nach der verfügbaren Eigenkapitaldecke und einem Sicherheitszuschlag für Unsicherheiten. Der Wert der Assets, welche einem Downsiderisk ausgesetzt und damit potentiell in Gefahr sind, werden auch unter dem Begriff ‚Value at Risk' subsummiert. Siehe hierzu auch die unten folgenden Ausführungen.

Werden mit Chancen verbundene Gefahren mit einem präzisen Risikomanagement adäquat unter Kontrolle gehalten, so kann die Unternehmung grössere Downsiderisiken eingehen und damit ein Maximum an Chancen antizipieren, ohne sich existenzgefährdenden Gefahren auszusetzen. Je besser das Risikomanagement einer Unternehmung, desto mehr Risiken können eingegangen werden. Erhöhte Upsiderisks, daher Chancen, können im Business gewinnbringend ausgebeutet werden. Abbildung 3 veranschaulicht diese Situation. Idealisierend kann die Unternehmung durch ein perfektes Risikomanagement den Sicherheitszuschlag auf

[13] [UBSOUTLOOK01]

Null reduzieren. In der Praxis kann der Sicherheitszuschlag verkleinert werden. Anstelle von höheren Risiken kann auch das notwendige, teure Eigenkapital minimiert werden. Diese Situation dürfte vor allem bei Banken von Bedeutung sein.

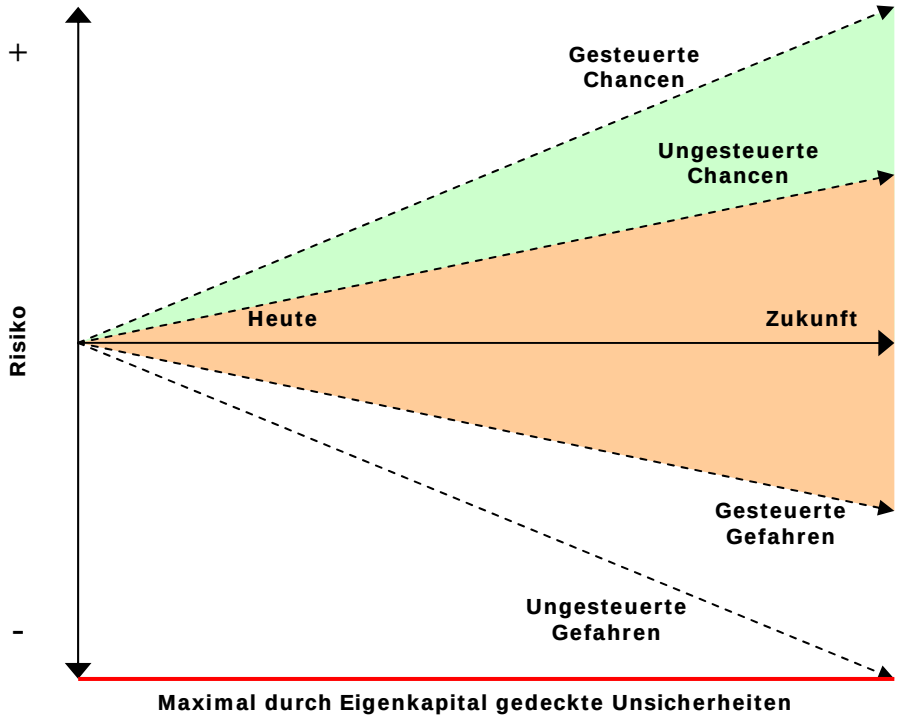

Abbildung 3: Risikomanagement erlaubt höhere Risiken

Value at Risk[14]

Im Abschnitt 3.1.5 wurde zum Schluss die Eigenkapitalabdeckung von Risiken erwähnt. Eigenkapital ist eine monetäre Grösse, der Risikomanger ist daher interessiert seine Risiken ebenso monetär auszudrücken. Dies leistet genau das Konzept des Value at Risk. Im folgenden soll dieser deshalb kurz gezeigt werden.

Der englische Begriff Value at Risk (VaR) bedeutet sinngemäss: ‚Wert auf dem Spiel'. Basierend auf einem mathematisch-statistischen Verfahren wird das Verlustpotential aus einem Geschäft oder einer Aktivität berechnet. Für einzelne Geschäfte sind VaR Kennzahlen nur beschränkt aussagekräftig. Interessanter ist die Analyse eines Portefeuilles, hier ist eine statistische Betrachtung eher sinnvoll. Häufig werden VaR Ansätze bei der Analyse von Finanzinstrumenten angewendet, der Anwendung auf andere Bereiche, z.B. für Projektportfolios oder Betriebsrisiken, steht aber nichts im Wege.

[14] [DEMPSTER02]

Hauptaufgabe des VaR ist die adäquate Aggregation aller Gefahren zu einer Kennzahl. Die Hauptschwierigkeit besteht darin, die Dichtefunktion oder die Verteilung des jeweils individuellen Portefeuilles festzulegen. Ausgangspunkt ist dabei häufig auch hier die Gauss'sche Normalverteilung.

3.1.6 Ziele des Risikomanagements[15]

Unternehmen müssen sich Chancen schaffen um zu überleben. Je mehr Chancen eine Unternehmung zur Verfügung hat, desto grösser ist der Handlungsspielraum und damit die Möglichkeiten erfolgreicher zu sein. Die Hauptziele des Risikomanagements sind die Fragen nach dem (a) wie viele Risiken und (b) welche Risiken eingegangen werden sollen, sowie der Optimierung derselben. Chancen sollen maximiert und Gefahren minimiert werden. Das Risikomanagement bietet Tools und Konzepte zu effizienten und effektiven Erledigung dieser Aufgabe.

3.1.7 Voraussetzungen für Risikomanagement

Risikobewusstsein

Mangelndes Risikobewusstsein setzt Unternehmen unnötigen Gefahren aus und verhindert die Antizipation von Chancen. Der verfügbare Handlungsspielraum wird nicht effizient ausgenutzt, was zunehmend ein Wettbewerbsnachteil ist. Risikobewusstsein setzt auch Kenntnisse der fundamentalen Risikokonzepte voraus. Diese müssen in Form von Weiterbildung vermittelt werden. Erst aus dieser Basis kann ein Risikobewusstsein entstehen.

Risikokultur

Neben dem Risikobewusstsein muss eine explizite Risikokultur gelebt werden. Entsprechende Kompetenzen sind z.B. durch Fortbildung sicherzustellen. Das Unternehmen muss bereit sein, kalkulierte Risiken einzugehen und gleichzeitig fähig sein, diese Risiken auch tragen zu können. Teil einer Risikokultur ist auch eine Risikopolitik in welcher z.B. festgelegt ist, welche Risiken bis zu welchem Ausmass eingegangen, vermieden, vermindert, abgewälzt oder selber getragen werden sollen. Entscheidend ist dabei die Fähigkeit, unerwartete Verluste durch Eigenmittel abzudecken und erwartete Verluste über Risikoprämien auszugleichen.

[15] [FIGLEWSKI02]

3.1.8 Der Risikoprozess

Die Beurteilung der Risiken folgt meistens dem gleichen, hierarchischen Schema. Dieser Risikoprozess ist in Abbildung 4 entsprechend aufgeführt. Beginnend mit der Identifikation von Risiken bis zur Risikokontrolle. Die *Risikoidentifikation* sucht nach möglichen Risiken und versucht diese explizit zu machen. Es ist dabei zu betonen, dass im strengen Sinne von Risikomanagement damit auch Chancen gemeint sind. Meistens ist die Identifikation von Risiken auf Gefahren beschränkt. Die Chancen werden im Business gesucht. Sind die Risiken gefunden, wollen diese analysiert werden, damit die nachfolgende Beurteilung möglich wird. Je mehr Informationen bei der *Risikoanalyse* gesammelt werden können, desto besser wird in der Regel die Risikohandhabung sein. Oft lassen sich Risiken nur schlecht quantifizieren, die *Risikoquantifizierung* wird daher gerne vernachlässigt. Trotzdem interessiert zum Schluss ein Betrag, welcher das Risiko wiederspiegelt. Ist das Risiko beurteilt und quantifiziert, können geeignete Strategien beschlossen werden, wie das Risiko in einer optimalen Weise *gehandhabt* wird. Zum Schluss sollte eine Kontrolle stattfinden, welche den Risikoprozess auf sein Funktionieren hin *kontrolliert*. Risikomanagement ist kein statischer, einmaliger Prozess. Risikoeinschätzungen altern schnell und verlieren dabei an Relevanz und Aussagekraft. Der Risikokontrolle folgt daher zyklisch wieder die Risikoidentifikation.

Abbildung 4: Der Risikoprozess

3.1.9 Quantifizierungsstrategien

Sind Bereiche mit möglichen Risiken identifiziert und wurden diese einer genaueren Analyse unterzogen, wollen die Risiken einer Quantifizierung unterzogen werden. Dazu existieren verschiedene Ansätze. Generell gilt jedoch, je mehr Informationen und je höherwertiger diese sind, desto besser kann das Risiko quantifiziert werden.

3.1.9.1 Risikoquantifizierungen sind Prognosen

Wären Risikoabschätzungen nur auf das Hier und Jetzt bezogen, würden die durch Risiken bestehenden Chancen bereits Gewinne generieren oder Gefahren Verluste produzieren. Die Idee des Risikos ist aber eine Aussage über zukünftige Ereignisse. Je weiter ein Ereignis in der Zukunft liegt, desto grösser werden die Unsicherheiten und damit das Risiko. Abbildung 5 verdeutlicht diesen Zusammenhang.

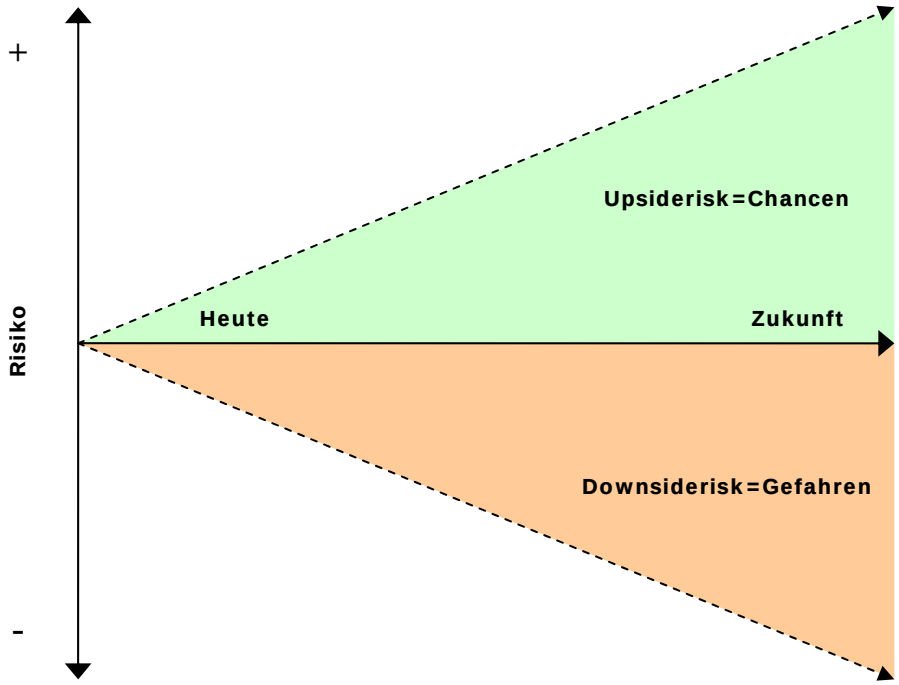

Abbildung 5: Zusammenhang Risiko und Zeit

3.1.9.2 Unsicherheit versus Risiko

In der Literatur wird häufig zwischen den Begriffen ‚Unsicherheit' und ‚Risiko' unterschieden. ‚Unsicherheit' bezeichnet dabei zukünftige Ereignisse über deren Eintretenswahrscheinlichkeit nichts bekannt ist. Als ‚Risiko' werden Ereignisse in der Zukunft bezeichnet, zu welchen Eintretenswahrscheinlichkeiten bekannt sind oder geschätzt werden können. Mit Risiken lässt sich im Gegensatz zu Unsicherheiten rechnen. Dabei müssen Risiken nicht spezifische Zahlenwerte zugeordnet sein. Bereits Risikoreihenfolgen lassen begrenzte Berechnungen zu. Bei genauerer Betrachtung lässt sich jede Unsicherheit durch Analyse und Quantifizierung in ein Risiko überführen. Spiegelbildlich lassen sich Risiken durch Falsifizierung der zugeordneten Zahlenwerte in eine Unsicherheit überführen. Das Problem zielt auf die Frage ab, ob die Folgen gewisser Ereignisse in der Zukunft überhaupt hinreichend präzise abgeschätzt werden können. Wenn eine Schätzung vorgenommen wird, ist unklar ob diese auch wirklich Relevanz hat. Dies ist ein grundsätzliches Problem der Prognose. Die Richtigkeit von Prognosen lässt sich immer nur im Nachhinein zeigen. Die genauere Behandlung dieser Frage soll hier aber nicht weiter aufgeführt werden.

3.1.9.3 Schätzer

Schätzungen lassen sich grob in drei Verfahren einteilen. Die Punktschätzung ist das meistverbreitete und auch einfachste Verfahren. Ein wenig komplexer ist die

Szenarioanalyse, verschiedene Szenarien werden dabei gegenübergestellt. Das komplexeste und gleichzeitig ergiebigste Schätzverfahren ist die Modellierung einer Wahrscheinlichkeitsverteilung. Im Folgenden werden diese drei Verfahren kurz erläutert.

Punktschätzung

Bei der Beurteilung von Risiken muss einerseits das mögliche finanzielle Ausmass bestimmt werden als auch die Wahrscheinlichkeit, dass dieser Schaden überhaupt eintritt. Diese Vorgehensweise entspricht der oben angegebenen Formel 1. Dabei handelt es sich um eine einfache Punktschätzung. Weder über die Verteilung des Schadensausmasses noch über die Verteilung der Eintretenswahrscheinlichkeit wird etwas ausgesagt. Die Punktschätzung ist das einfachste Schätzverfahren. Ein Abteilungsleiter kann z.B. schätzen, dass mit 50% Sicherheit ein Bereichsumsatz von 5 Mio. erreicht wird. Weitergehende Aussagen sind ohne weitere, explizite Schätzung nicht möglich. Statistisch ausgedrückt handelt es sich dabei meistens um den Modalwert der zugrundeliegenden aber unbekannten Verteilung. Der Modalwert ist nicht zu verwechseln mit dem Modus, der angibt welcher Wert am häufigsten vorkommt. Wird eine Punktschätzung gemacht, ist davon auszugehen, dass Modus und Modalwert nicht auseinandergehalten werden, liegen doch beide Werte oft nah beisammen.

Szenarien

Ein wenig komplexer ist die Bildung von Szenarien. Im Gegensatz zur Punktschätzung, wo globale Annahmen getroffen werden, können bei Szenarien einzelne Konstellationen von Annahmen durchgespielt werden. Die Aggregation der Szenarien ergibt eine simple Verteilungsfunktion. Je mehr Szenarien aggregiert werden, desto präziser wird die Verteilungsfunktion. Bei der Aggregation müssen die einzelnen Szenarien mit einer eigenen Eintretenswahrscheinlichkeit versehen werden. Der oben erwähnte Abteilungsleiter könnte also 2 Szenarien aufstellen, eines sieht den Markteintritt eines Mitbewerbers vor, das andere nicht. Beide Szenarien ergeben einen anderen Erwartungswert für den Gewinn. Der Markteintritt selber muss aber auch mit einer Eintretenswahrscheinlichkeit versehen werden. In der unten aufgeführten Abbildung 6 wurde angenommen, dass jedes Szenario ebenfalls normalverteilt ist, und dass beide Szenarien gleich wahrscheinlich sind. Die

Aggregation muss normalisiert werden, so dass das Integral wieder 1 wird. Der Erwartungswert der Gesamtschätzung liegt immer noch bei 5 Mio., die Analyse der Verteilung lässt aber weitergehende Schlüsse zu. Es ist zum Beispiel ersichtlich, dass der Schwankungsbereich des erwarteten Gewinnes recht gross ist. Eine einzige Punktschätzung hätte das nicht vermocht. Szenarien lassen sich auch als einzelne Punktschätzungen bewerten. Die Aggregation ist dann allerdings nicht so einfach möglich.

Ein Spezialfall des Szenarioverfahrens ist die Bildung von 3 Szenarien, eines für den schlechtesten Fall (*worst case*), eines für den wahrscheinlichsten Fall (*most likely*) sowie eines für den besten Fall (*best case*). Die beiden Randszenarien bilden Extremsituationen ab, über deren Eintretenswahrscheinlichkeit aber nichts weiter bekannt ist. Deren Aussagekraft ist daher fragwürdig. Der most likely Fall ist nichts weiter als eine Punktschätzung.

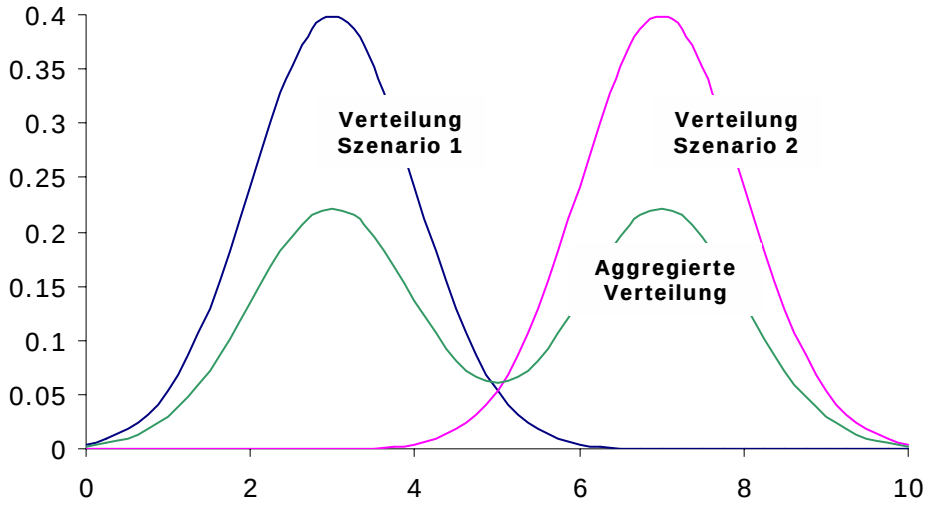

Abbildung 6: Aggregation von Szenarien

Verteilungsmodellierung

Die anspruchvollste Vorgehensweise bei der Schätzung ist die Bestimmung einer geeigneten Verteilung. Die Verteilungsfunktion spiegelt die Aggregation aller Szenarien. Da nie alle Szenarien durchgerechnet werden können und die dazu notwendigen Parameter ins grenzenlose wachsen würden, ist die gewählte Verteilungsfunktion meistens ein Kompromiss.

Oft wird bei Unkenntnis über die wahre Verteilung die unten in Abbildung 7 gezeigte Normalverteilung gewählt. Diese steht für ein beliebiges Ereignis X, z.B. die bereits oben erwartete Gewinnentwicklung einer Abteilung. Auf der X-Achse könnte dann der erwarte Gewinn einer Abteilung stehen. Die Y-Achse zeigt die Dichtefunktion der zugrunde liegenden Verteilung. Die Fläche unter der Kurve entspricht 1, d.h. das Ereignis tritt sicher ein. Eine Punktschätzung macht nun die Aussage, dass z.B. der Umsatz von mindestens 5 mit einer Wahrscheinlichkeit von 0.5 erreicht wird. Diese Schätzung wird in der Normalverteilung mit einer Fläche der Grösse 0.5 dargestellt. Da der Umsatz mindestens 5 Mio. ein muss, ist damit die Fläche unter dem rechten Teil der Kurve gemeint. Bei der Punktschätzung liegen dann keinerlei weitere Informationen über die Verteilung dieser Gewinnerwartung vor. Dies im Gegensatz dazu, wenn die Verteilung modelliert wird, z.B. als Normalverteilung. Ein weiterer Vorteil einer Modellierung der Verteilung liegt darin, dass Fragestellungen möglich sind wie „wie gross ist die Wahrscheinlichkeit, dass der Umsatz unter 2 Mio. bleiben wird“.

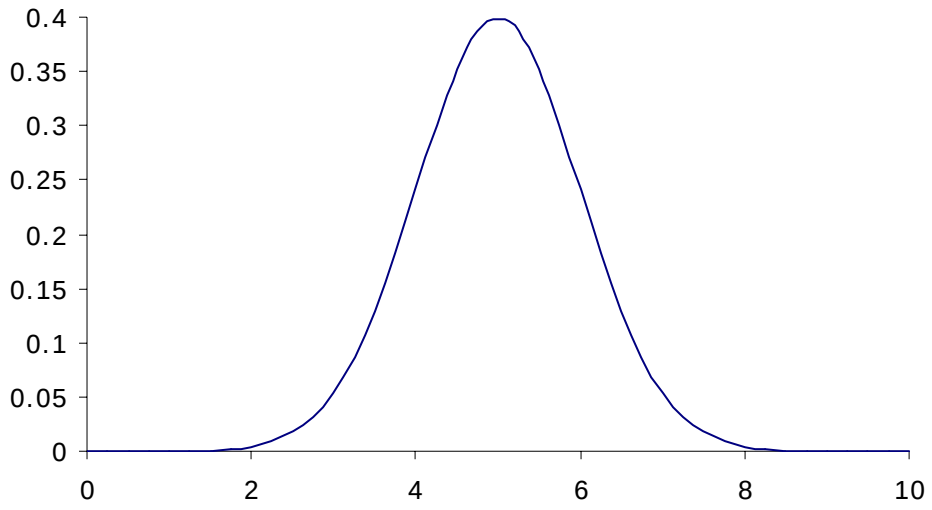

Abbildung 7: Verteilung eines Ereignisses (Normalverteilung)

Soll die Verteilung eines Ereignisses bestimmt werden, so kann dabei oft auf keine externen Variabeln zurückgegriffen werden. So ergibt sich eine Verteilung ‚aus dem Bauch', die Aussagekraft ist dabei nicht viel grösser als bei einer Punktschätzung. Bessere Resultate werden erreicht, wenn versucht wird, ein Modell mit möglichst vielen aussagekräftigen unabhängigen Variabeln zu erstellen. Die unabhängigen Variablen werden dabei wiederum mit einer Verteilung versehen. Über diese

Variablen mit definierten Verteilungen wird eine Simulation gefahren. Dabei wird bei jedem Durchgang allen unabhängigen Variabeln ein Zufallswert zugewiesen, welcher der jeweils angegebenen Verteilung entspricht. Die Aggregation aller Simulationswerte ergibt die Verteilung des Ereignisses. Dieses Verfahren generiert n (n=Anzahl Simulationsdurchgänge) Szenarien. Da es auf einer reinen Zufallsauswahl der Inputvariabeln basiert, wird diese Verfahren auch Monte Carlo Simulation genannt[16]. Die Wahrscheinlichkeit der einzelnen Szenarien ist gleich. Dazu und zu weiteren Verfahren bestehen diverse Softwarelösungen. Neben einer Simulation wäre auch eine mathematische Aggregation der Szenarien möglich. Die Auswahl aus der unendlichen Menge an möglichen Szenarien muss aber trotzdem nach Zufallsprinzipien erfolgen.

3.1.10 Handhabungsstrategien[17]

Sind Risiken erkannt und quantifiziert, muss der Entscheid gefällt werden, wie die Risiken gehandhabt werden soll. Folgende Vorgehensweisen sind dabei möglich:

Prävention

Besteht die Möglichkeit, Gefahren einfach zu verhindern, ist die Risikoprävention sinnvoll. Prävention ist nicht immer möglich, speziell in den Situationen, bei welchen nicht alles unter der Kontrolle der Unternehmung ist.

Generierung

Die bewusste Generierung von Risiken erscheint auf den ersten Blick wenig angebracht. Sobald mit den Risiken aber Chancen gemeint sind, erhält die Generierung von Risiken eine durchaus sinnvolle Dimension. Wie Gefahren durch einfache Massnahmen verhindert werden können, ist es auch möglich, Chancen mit geringem Aufwand zu schaffen.

Kauf/Verkauf

Der Vorteil vom Kauf/Verkauf von Chancen oder Gefahren liegt in der objektiven Bewertung. Das Risiko wird dabei durch einen Preis vollständig einer anderen Organisation übertragen.

[16] Die Frage, ob bei Montecarlo alles nach Zufall abläuft soll hier nicht beantwortet werden.
[17] [BORGE01]

Diversifizierung

Durch Diversifizierung eines Portfolios kann das Gesamtrisiko vermindert werden. Dabei wird die Anzahl der Portfolioelemente vergrössert. Diversifizierung lässt sich bei allen Arten von Portfolios wie Projektportfolios, Applikationsportfolios oder Wertschriftenportfolios betreiben. Der Nachteil der Diversifizierung besteht darin, dass dabei parallel Upsiderisk und Downsiderisk vermindert werden. Ein diversifiziertes Portfolio bietet nicht mehr die gleichen Chancen wie ein homogenes Portfolio.

Konzentration

Die Konzentration von Gefahren vermindert die damit verbundenen Risiken nicht automatisch. Aber die Steuerung von geeigneten Massnahmen zur Minimierung der Gefahren wird erleichtert. Auch die Konzentration von Chancen lässt diese besser nutzen.

Hedging

Als Hedging wird der Mechanismus verstanden, ein Risiko durch ein anderes, entgegenwirkendes Risiko zu kompensieren. Aus der Finanztheorie sind dabei perfekte und imperfekte Hedges denkbar. Beim perfekten Hedge ist das Ausmass des Grundrisikos und des Gegenrisikos gleich gross, beim imperfekten nur partiell.

Leveraging

Durch geeignete Hebel wird die Wirkung eines Risikos noch verstärkt. Dies ist einerseits in der Finanzindustrie interessant, kann aber auch durchaus im IT-Risikomanagement Sinn machen. Bestehen zum Beispiel die Chancen auf einen Produkterfolg, so kann dieser durch geeignete Massnahmen noch verstärkt werden. An einem Leveraging von Gefahren besteht meistens kein Interesse.

Versicherung

Eine der verbreitetsten und wirkungsvollsten Strategien, Risiken zu handhaben, ist die Versicherung. Meist wird nur das Downsiderisk versichert. Aber auch der umgekehrte Weg wäre denkbar. Wird das Risiko vollständig versichert, so kommt man dem Verkauf des Risikos sehr nahe. Ein Vorteil der Versicherung ist wie beim Verkauf die objektive Bewertung des Risikos durch einen Preis. Allerdings bedeutet

Objektivität noch lange keine Transparenz oder Richtigkeit. Eine zu tiefe Versicherung kann zu falscher Sicherheit verleiten.

3.1.11 Einsatzgebiete des Risikomanagements

3.1.11.1 Ursprung des betrieblichen Risikomanagements

Risikomanagement wurde bei Finanzdienstleistern zuerst eingeführt und ist dort heute stark verbreitet. Dort sind die Risiken der gehandelten Finanzinstrumente zentral und relativ einfach berechenbar. Dazu bestehen äusserst ausgeklügelte Theorien.

3.1.11.2 Risikomanagement in der IT

Weniger in diesem Geiste des Risikomanagements analysiert werden Risiken, welche sich auf IT-Spezifische Handlungen einer Unternehmung beziehen. Dazu zählen die Bereiche wie sie in Abbildung 8 dargestellt sind[18]. Die rechten Bereiche halten die Unternehmung am laufen („running the copmpany“), auf der linken Seite wird die Unternehmung verändert („changing the company“).Weitere Teilbereiche wie z.B. Marktrisiken oder Compliance Risiken sollen in dieser Arbeit nicht betrachtet werden, gehören aber selbstverständlich auch zu einem umfassenden Risikomanagement.

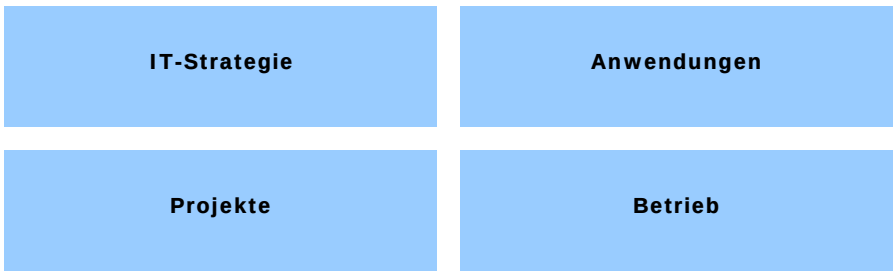

Abbildung 8: Bereiche des Risikomanagements

3.1.11.3 IT-Strategie

Aus der Festlegung der IT-Strategie ergeben sich spezifische Risiken. Seite an Seite mit dem IT-Controlling müssen diese Risiken erkannt, analysiert, quantifiziert und gehandhabt werden. In der IT Strategie werden die Rahmenbedingungen festgelegt, wie sich die IT der Unternehmung mittel bis langfristig entwickeln soll. Zwei Sichtweisen sind dabei dominierend: „running the company“ und „changing the company“. Aus diesen Sichtweisen ergeben sich die weiteren Teilaspekte der IT-

[18] in Anlehnung an [GYSLER95]

Strategie. Diese können sein eine geplante Konzentration auf eine Mainframe-Platform, der Einsatz von einheitlichen Desktopbestriebssystemen oder die Umsetzung eines speziellen Projektvorgehensmodells.

Aus der Festlegung der IT-Strategie verspricht sich die Unternehmung strategische Wettbewerbsvorteile und handelt sich gleichzeitig Risiken und Kosten ein. Wettbewerbsvorteile können unter dem Konzept des Risikomanagements auch als Upsiderisk oder Chancen interpretiert werden. Massnahmen, welche zu Chancen führen implizieren aber meistens auch gewisse Gefahren, eben das Downsiderisk. Damit sich die Unternehmung nicht ungewollten Risiken aussetzt, sei das nicht vorhandene Risikobereitschaft oder mangelnde Risikofähigkeit durch eine zu geringe Eigenkapitaldecke, muss ein Risikomanagement auch die strategischen Risiken unter Kontrolle halten.

3.1.11.4 Anwendungen

Anwendungen sind IT-Dienstleistungen, welche von internen Nutzern beansprucht werden. Dazu gehören Desktopsystem, Reportingtools, Mailsystem, Netzinfrastruktur, Helpdesk oder Drucksystem. Der Bereich Anwendungen wird manchmal auch unter dem Begriff Infrastruktur subsummiert, die Begriffe sind aber nicht deckungsgleich. Aus dem Einsatz dieser Systeme ergeben sich Risiken. So hat der Ausfall des Drucksystems Ausfallskosten und unzufriedene Kunden zur Folge. Eine Fehlfunktion im Mailsystem kann fatale Folgen für eine Kundenbeziehung haben. Das Risikomanagement muss sicherstellen, dass Anwendungsrisiken unter Kontrolle sind und in optimaler Weise gesteuert werden.

3.1.11.5 Projekte

Projekte verursachen Kosten, verändern die Unternehmung und generieren Chancen und Gefahren. Risikomanagement bei Projekten ist daher vielschichtig. Das Risikomanagement muss sicherstellen, dass die Kosten nicht die erwarteten Chancen welche man sich durch das Projekt verspricht übersteigen. Da Projekte Unternehmen stark verändern können, zum Beispiel durch die Einführung neuer Transaktionssysteme, müssen erstens die damit verbundenen Gefahren speziell untersucht werden. Zweitens darf natürlich die Untersuchung erwarteter Chancen nicht vergessen werden. Die erste Aufgabe erledigt meistens das klassische

Risikomanagement. Die zweite Aufgabe wird oft in Form einer Wirtschaftlichkeitsanalyse erledigt.

Neben den Risiken, welche von einzelnen Projekten ausgehen, ist die Frage nach dem gesamten Projektportfoliorisiko interessant. Sind die Risiken der einzelnen Projekte bekannt, können diese aggregiert werden. Damit das funktioniert, werden einheitliche Beurteilungsgrundlagen benötigt, ansonsten werden ‚Äpfel mit Birnen' verglichen.

Das Risikomanagement muss für Projekte sicherstellen, dass Projektrisiken unter Kontrolle sind und in optimaler Weise gesteuert werden.

3.1.11.6 Betrieb

Der Informatikbetrieb stellt Transaktionssysteme und Speichersysteme für die Abwicklung des Business zur Verfügung. Der Informatikbetrieb ist von einer grossen Systemvielfalt, bestehend aus verschiedener Hardware und Software geprägt. Mit dem Betrieb sind Risiken verbunden. Wichtige Risiken sind Sicherheitsmängel und Verfügbarkeiten. Aber auch Fehlfunktionen und mangelnde Wirtschaftlichkeit sind Risiken.

Aufgabe des Risikomanagements für den Betrieb ist die Sicherstellung, dass Betriebsrisiken unter Kontrolle sind und in optimaler Weise gesteuert werden.

3.1.12 Anforderungen aus BASEL II/KonTraG

3.1.12.1 KonTraG

Spektakuläre Unternehmenszusammenbrüche führten zu zunehmender Kritik an geltenden Überwachungssystemen für Kapitalgesellschaften. Sowohl die Wirksamkeit der internen Revision, die Prüfung der Geschäftsführung durch den Aufsichtsrat, als auch die Intensität und Aussagekraft einer Jahresabschlussprüfung wurden in Frage gestellt. Als eine der Konsequenzen dieser Kritik trat in Deutschland am 1.5.1998 das „Gesetz zur Kontrolle und Transparenz im Unternehmen" (*KonTraG*) in Kraft. Es beinhaltet Neuerungen für die Organe des Unternehmens hinsichtlich Überwachung

und Berichterstattung, aber auch für den Jahresabschlussprüfer hinsichtlich Prüfung und Prüfungsbericht.[19]

3.1.12.2 BASEL II

Ende 1992 trat das Abkommen Basel I zur Eigenkapitaldeckung in Kraft. Zu BASEL II besteht zur Zeit ein drittes Konsultationspapier, das Inkrafttreten des Abkommens ist aber erst per 2006 geplant. Beide Abkommen regeln die Ausgestaltung des Eigenkapitals bei Banken. Der Schwerpunkt liegt dabei auf international tätigen Banken, ihre Grundsätze sollen sich aber auch für die Anwendung auf Banken unterschiedlicher Komplexität und unterschiedlich anspruchsvoller Tätigkeit eignen. Dabei werden Bereiche wie Kredit-, Markt-, Liquiditäts- und anderen Risiken abgedeckt. Die neue Regelung sieht bei der Bestimmung der notwendigen Eigenkapitalquote eine Reihe von einfachen und fortgeschritteneren Ansätzen zur Messung des Kreditrisikos und des operationellen Risikos vor. Der Bereich der operationellen Risiken kann für Unternehmen jeglicher Couleur angewandt werden.

3.1.12.3 Relevanz von KonTraG und BASEL II

Das KonTraG sowie BASEL II richtet sich eher an den Vorstand und die Organe der Kapitalgesellschaft. BASEL II richtet sich primär an Finanzinstitute. Die Relevanz für die vorliegende Arbeit ist also nicht sofort ersichtlich. Da übergeordnete Organe auf sinnvolle Daten aus dem Business angewiesen sind, ist mit dem Gesetz auch das Controlling und das Risikomanagement betroffen. Ist die IT im Unternehmen eine Kernfunktion wie bei Banken, ist zwangsläufig auch das IT-Controlling sowie das IT-Risikomanagement von verschärften Anforderungen aus KonTraG oder Basel II betroffen. Der Geist von Basel II sowie eines KonTraG unterstreichen daher die Wichtigkeit der Aufgaben von IT-Controlling und IT-Risikomanagement. Eine spezifische Anforderung aus Basel II und KonTraG ist das Vorhandensein eines funktionierenden IT-Controllings und, wo noch nicht überall wirksam eingeführt, ein IT-Risikomanagement.

[19] In Anlehnung an [LEGAMEDIA]

3.2 IT Controlling[20]

3.2.1 Controllingbereiche

Für das IT-Controlling muss das gleiche gelten wie für das Controlling im Allgemeinen: „Jeder hat seine eigene Vorstellung darüber, was Controlling bedeutet oder bedeuten soll, nur jeder meint etwas anderes“[21] Trotzdem soll hier versucht werden, das Gebiet des IT-Controlling einzugrenzen.

Die primären Tätigkeitsgebiete des IT Controlling gliedern sich grob in vier Bereiche[22]:

- Strategisches IT Controlling[23]
- Projektcontrolling
- Betriebscontrolling
- Anwendungscontrolling

Diese Einteilung entspricht genau der Einteilung für das Risikomanagement aus 3.1.11.2 wie sie in der Abbildung 8 dargestellt sind. Dies ist auch sinnvoll da die meisten Elemente, welche für das IT-Controlling von Interesse sind, auch das IT-Risikomanagement interessieren.

Im IT-Controlling hat das Projektcontrolling eine überragende Bedeutung. Dazu existiert diverse Literatur. Das Betriebscontrolling erfolgt oft über SLA’s[24].

3.2.2 Abweichungsanalyse

Neben unterstützenden Funktionen hat das Controlling die Abweichungsanalyse zum Gegenstand. Die Abweichungen sollen aufgezeigt und transparent gemacht werden. Zur Transparenz gehört auch das Aufzeigen von Risiken, welche durch Abweichungen verursacht werden. Was mit diesen Informationen passiert, ist dann Sache der Unternehmensführung.

[20] [BURGER02]
[21] [PREISSLER98]
[22] in Anlehung an [GYSLER95]
[23] [HEILMANN01]
[24] Akronym für ‚Service Level Agreement’

3.2.3 Typen von Controlling

Neben den Tätigkeitsgebieten lässt sich Controlling in *operatives* und *finanzielles* Controlling aufteilen. Das operative Controlling beschäftigt sich mit nicht finanziellen Grössen und steht in direktem Bezug zur Leistungserstellung. Im Gegensatz dazu beschäftigt sich das finanzielle Controlling mit den finanziellen Kenngrössen und der Leistungsverrechnung

Dominant waren und sind noch heute finanzielle Informationen. Dies speziell im strategischen IT Controlling. In jüngster Zeit halten aber vermehrt auch nicht finanzielle Informationen Einzug, z.B. in Form einer Balaced IT-Score Card.

Jedes Controlling benötigt Datenquellen und verarbeitet diese mittels geeigneten Instrumenten. Dabei fällt die Trennung zwischen Datenquelle und eingesetztem Instrument oft schwer. Daten werden bereits mit Instrumenten erfasst und unterliegen damit bei der Erfassung bereits einer Kontrolle und damit Beeinflussung. Trotzdem soll im folgenden versucht werden, Quellen der Informationsversorgung von Instrumenten losgelöst zu betrachten.

3.2.4 Informationsquellen[25]

Die in Tabelle 1 aufgeführten Informationsquellen demonstrieren eine grosse Heterogenität der Datenquellen. Oft ist der Bedarf an Informationen nicht aus diesen Quellen direkt beziehbar. In diesen Fällen werden mit Hilfe von Office Produkten wie Excel oder Access die gewünschten Daten zusammengestellt. Dabei entstehen Medienbrüche, manuelle Datenübertragungen oder Dateninkonsistenzen[26]

Informationsquelle	Beschreibung
externe Rechnungslegung	Nach Aussen publizierte Informationen über die Unternehmung, meist finanzieller Natur, in zunehmendem Masse aber auch nicht finanzielle Daten. Diese Daten liegen primär in Form von Geschäftberichten vor. Aber auch Berichte zuhanden der Steuerverwaltung, Aktionärsgruppen oder Börse sind denkbar. Die Formate sind hier eher heterogen, die Datenmenge dafür weniger umfangreich.
Finanzrechnung	Die Finanzrechnung wird auch als Liquiditätsrechnung bezeichnet. Ein Unternehmen ist liquide, wenn es in der Lage ist, Zahlungsverpflichtungen nachzukommen. Zweck der Finanzrechnung ist die Beschaffung und Anlage von Kapital.

[25] in Anlehnung an [WEBER99]
[26] [FRÖHLING00]

Informationsquelle	Beschreibung
	Diese Daten liegen in der Form der verwendeten Tools vor. Das kann z.B. ein SAP System sein.
Investitionsrechnung	Die Investitionsrechnung beschäftigt sich mit der Kalkulation von Investitionen. Dabei werden grundsätzlich die Einzahlungen und Auszahlungen einer Investition gegenübergestellt, um die Wirtschaftlichkeit verschiedener Investitionen zu beurteilen. Die Problematik besteht darin, dass die Erwartungen über zukünftige Einzahlungen, tatsächliche Nutzungsdauer und zukünftige Investitionsmöglichkeiten risikobehaftet sind. Auch diese Daten liegen in Form der verwendeten Tools vor.
Kostenrechnung	Die Kostenrechnung stellt sicher, dass alle Kosten der IT erfasst und den Leistungsträgern gutgeschrieben beziehungsweise den Leistungsbezügern verrechnet werden. Die Verrechnung erfolgt auf Basis der Leistungsdaten der Leistungsrechnung. Kosten Bei der Verrechnung kommen die Verfahren der Kostenartenrechnung und Kostenstellenrechnung zum Einsatz. Kosten können auf Basis der Vollkosten, Teilkosten oder der betrieblichen Prozesse verrechnet werden. Daten kommen dabei aus den Kostenrechnungsapplikationen, diese können z.B. SAP Systeme sein.[27]
Leistungsrechnung	Die Leistungsrechnung erfasst die erbrachten Leistungen der IT und bewertet sie mit Preisen oder durch Zurechnung von Kosten. Die Leistungsrechnung ermöglicht weiter die Planung und Steuerung der aufgebauten Leistungen. Daten kommen dabei aus den Leistungsrechnungsapplikationen, diese können z.B. SAP Systeme sein.[28]
Erlösrechnung	Die Erlösrechnung ermittelt die Erlöse im Rahmen der internen Erfolgsrechnung. Dabei können losgelöst von den gesetzlichen Grundsätzen kalkulatorische Erlösbestandteile berücksichtigt werden, indem z. B. Tagespreise statt der effektiven Absatzpreise angesetzt werden. [29] Daten kommen dabei aus den Erlösrechnungsapplikationen, diese sind auch hier oft SAP Systeme.
Kennzahlensysteme	Ein Kennzahlensysteme ist eine geordnete Gesamtheit von betriebswirtschaftlichen Kennzahlen, die in einer sinnvollen Beziehung zueinander stehen. Als Gesamtheit informieren sie in konzentrierter Form über betriebswirtschaftliche Sachverhalte. Der rechnerische Aufbau erfolgt vielfach in Form einer pyramidalen Abstufung. Analytische Kennzahlensysteme entstehen durch Zerlegung einer Spitzenkennzahl in Unterkennzahlen. Synthetische Kennzahlensysteme entstehen durch Verdichtung mehrerer Einzelkennzahlen zu einer Spitzenkennzahl. Kennzahlen können teilweise Betrieblichen Applikationen entnommen werden. Je weiter unten in der Hierarchie oder je weniger Finanznah die Kennzahl ist, desto mehr kommen dabei heterogene Systeme zum Einsatz. Oft werden Kennzahlen Ad-hoc z.B. in Excel berechnet.
externe Daten	Neben internen Zahlen sind externe Informationen sowohl für das langfristige Überleben als auch z.B. für das schnelle Reagieren auf Marktveränderungen unabdingbar. Die Erfassung solcher Zahlen erfolgt oft in wenig strukturierter Form oder nur zentral. Oft werden externe Daten grösstenteils Teil durch die Salesforce erfasst und dies meistens nicht in weiter einsetzbarer expliziter Form. Die Datenquellen, sofern überhaupt vorhanden, sind Informationsbroker, die Salesforce oder sonstige

[27] in Anlehnung an [WEBER02]
[28] in Anlehnung an [WEBER02]
[29] in Anlehnung an [LEGAMEDIA]

Informationsquelle	Beschreibung
	unstrukturierte Informationsquellen der Mitarbeiter.
Wissensdatenbanken	Unter Wissensdatenbanken fallen Sammlungen von Wissen zu spezifischen Gebieten, z.B. Marktforschung oder Technologieanalysen. Firmen wie IDC, Gartner, Forester, Jupiter Research oder die MetaGroup um nur einige zu nennen. Diese bieten Wissen zu spezifischen Themen gegen Bezahlung zur Verfügung- Solche Informationen sind meist mit Metainformationen versehen in Datenbanken gespeichert.
Implizites Wissen	Informationen über Risiken sind meistens nicht in expliziter Form vorhanden. Einschätzungen sind in den Köpfen verantwortlicher Mitarbeiter. Diese Wissen kann mit geeigneten Techniken explizit gemacht werden. Techniken dazu sind Interviews, Seminare oder Befragungen. Das so gewonnene Wissen kann explizit formuliert und mit den notwendigen Metainformationen zur Semantik versehen werden.

Tabelle 1: Informationsquellen für das IT-Controlling

3.2.5 Planungsinstrumente[30]

Wie bei den Informationsquellen ist auch die Menge verfügbarer Planungsinstrumente unübersichtlich gross und wenig einheitlich. Teilweise fungieren inhaltlich fast identische Instrumente unter unterschiedlichen Namen. Die in Tabelle 2 aufgelisteten Instrumente sind oft auch keine ausschliesslichen Controlling-Instrumente. Aber sie dienen dem Controlling Sachverhalte transparent und damit planbar zu machen.

Planungsinstrument	Beschreibung
SWOT-Analyse	Der Name kommt aus dem Englischen: Strengths and Weaknesses, Opportunities and Threats. Die SWOT-Analyse analysiert Chancen und Risiken, welche sich aus der Umwelt des Unternehmens ergeben und verbindet sie mit den unternehmenseigenen Stärken und Schwächen.
Erfolgsfaktorenanalyse	Die Erfolgsfaktorenanalyse kann als Teilgebiet der SWOT-Analyse betrachtet werden. Dabei werden aber nur die Stärken und die Chancen analysiert. Daraus ergeben sich die Erfolgspotentiale. Der fehlende Teil der Schwächen und Gefahren wird ausgeblendet.
GAP-Analysen	GAP-Analysen bedeutet zu Deutsch soviel wie „Lückenanalyse“. Sie ist ein Instrument der Strategischen Planung zur Früherkennung strategischer Lücken. Die erwartete Entwicklung wird der geplanten Entwicklung gegenübergestellt, dabei lässt sich eine mögliche Ziellücke erkennen. Die Lücke kann durch geeignete strategische Massnahmen geschlossen werden.
Shareholder-Value-Analyse	Die Shareholder-Value-Analyse (SVA) ist ein Werkzeug zur Beurteilung und Messung des Zukunftserfolgs von strategischen Geschäftsfeldern, Investitionen und Unternehmensstrategien. Die Beurteilung erfolgt aus Sicht der Eigentümer. Die Shareholder-Value-Analyse ist eine Art der Investitionsrechnungsverfahren.
Produktlebenszyklusanalyse (Life Cycle Analysis)	Die Produktlebenszyklusanalyse hat zum Ziel, Produkte oder Anwendungen über deren gesamten Lebenszyklus zu

[30] in Anlehnung an [WEBER02]

Planungsinstrument	Beschreibung
	analysieren. Dabei interessieren quantitativ die Wirtschaftlichkeit und Qualitativ die Auswirkungen auf andere Produkte oder Applikationen.
Erfahrungskurvenmodell	Das Konzept der Erfahrungskurve basiert auf der Annahme, dass die Gesamtkosten eines Produktes mit jeder Verdopplung der kumulierten Ausbringungsmenge gesenkt werden können. Das Erfahrungskurvenmodell kommt aus der Industrie, kann aber auch für Dienstleistungen angewandt werden.
Target Costing	Target Costing oder Zielkostenrechnung ist ein marktorientiertes Kostenmanagementkonzept. Der Preis wird marktgerecht festgelegt und darauf aufbauend die Kalkulation des Produktes vorgenommen.
Technologieportfolio-Analyse	Bei der Technologieportfolio-Analyse werden die eingesetzten Technologien in einer Matrix, dem Technologieportfolio, abgebildet. Dimensionen können zum Beispiel eigene Technologiekompetenz und Marktrelevanz sein. Mit dem Portfolio lassen sich differenzierte Handlungsempfehlungen für Technologiestrategien ableiten.
Investitionsrechnungen	Investitionsrechnungen haben zum Ziel, die Vorteilhaftigkeit einer Investition zu prüfen. Vorteile ergeben sich im Hinblick auf die Zielsetzung des Unternehmens. Optimale Investitionsprogramme können rechnerisch bestimmt werden.
Scoring-Modelle	Scoring-Modelle werden auch als Nutzwert-Modelle bezeichnet. Scoring-Modelle sind formalisierte Verfahren zur Entscheidungsfindung. In der Nutzwertanalyse wird ein Punktwert für alle in Frage kommenden Vorhaben ermittelt. Dieser Punktwert ist ein Indikator für das Ausmass der Erfüllung der Unternehmensziele und damit für den Nutzen eines Vorhabens.
Benchmarking	Benchmarking ist das Vergleichen und Messens der eigenen Produkte, Dienstleistungen und Prozesse mit den besten Wettbewerbern oder mit den anerkannten Marktführern. Im Vergleich zum eigenen Unternehmen können Unterschiede festgestellt und Möglichkeiten zur Verbesserung aufgezeigt werden. Benchmarking bezieht sich auch auf Dienstleistungen und Prozesse.
Kostenvergleiche	Kostenvergleiche, seien es interne oder externe, sind effiziente Verfahren der Planung. Obwohl einfach im Konzept und Anwendung ermöglichen sie den Zugriff auf wichtige Informationen.
Deckungsbeitragsrechnungen	Zieht man vom Umsatz eines Produktes seine variablen Kosten ab, erhält man den Deckungsbeitrag. Der Deckungsbeitrag enthält also den Anteil am Umsatz für Fixkosten und Gewinn. Diese Information ist wichtig für kurzfristige Entscheidungen.
ABC-Analysen	Die ABC-Analyse ordnet zum Beispiel Kunden oder Kostenanteile aufgrund von mengen- und wertmäßigen Merkmalen in Kategorien. A-Kategorie: hoher Wert-, geringer Mengenanteil, B-Kategorie: mittlerer Wert- und Mengenanteil, C-Kategorie: geringer Wert- und hoher Mengenanteil. Ziel der ABC-Analyse ist es, die Ressourcen richtig aufzuteilen. ABC-Analysen werden auch in der Risikoanalyse eingesetzt.
Wirtschaftlichkeitsanalyse	Eines der wichtigsten Planungsinstrumente ist die Wirtschaftlichkeitsanalyse. Dabei wird die Wirtschaftlichkeitsanalyse meist Anfangs einer Investitionsentscheidung durchgeführt. Dabei müssen zukünftige, unsichere Erwartungen miteinbezogen werden. Für beliebige Objekte wie zum Beispiel Projekte, Produkte oder Infrastrukturen wird eruiert, ob es wirtschaftlich ist.

Planungsinstrument	Beschreibung
	Wirtschaftlich heisst dabei, dass investiertes Kapital zukünftig als Ertrag zurückfliesst.
Break-Even-Analyse	Ziel der Break-Even-Analyse ist primär die Ermittlung des Break-Even-Points. Voraussetzung ist dabei die Aufteilung der Kosten in Fixkosten und variable Kosten. Durch die Break-Even-Analyse erhält das Unternehmen Informationen über die Gewinnschwellenmenge. Das ist die Menge an verkauften Gütern, bei denen das Unternehmen einen ökonomischen Gewinn erwirtschaftet.
Kurzfristige Erfolgsrechnung	Die Kurzfristige Erfolgsrechnung folgt den gleichen Prinzipien der Erfolgsrechnung, ist aber unabhängig von steuer- oder handelsrechtlichen Bestimmungen.
Portfolio-Analyse	Ziel der Portfolio-Analyse im Marketing ist die Bestimmung eines Produkt-/ Marktprogramms unter Berücksichtigung zukünftiger Chancen und Risiken. Das Konzept kann aber auch für andere Bereiche angewandt werden.
Potentialanalyse	Die Potentialanalyse kann als Teil der SWOT-Analyse betrachtet werden. Wie bei der Erfolgsfaktorenanalyse werden dabei aus den eignen Stärken und bestehenden Chancen auf dem Markt entsprechende Potentiale eruiert.
Qualitätsmanagement und -Zirkel	Qualitätsmanagement umfasst die Tätigkeiten des Managements, die die Qualitätspolitik und die Ziele des Qualitätsmanagementsystems festlegen. Qualitätszirkel sind freiwillige Treffs von Mitarbeitern in einer formalen, d. h. nicht spontan organisierten Gruppe, um durch Erfahrungsaustausch die Qualität der zu verbessern

Tabelle 2: Planungsinstrumente IT-Controlling

Für die meisten Instrumente werden spezielle Softwaretools eingesetzt oder Firmenspezifische Microsoft Office Vorlagen verwendet. Je nach Analysetool werden nur wenige, bereits hochaggregierte oder sehr umfangreiche Inputdaten benötigt. Diese Daten kommen gemäss 3.2.4 aus den verschiedensten Quellen. Jede Quelle hat unterschiedliche Datenformate und behindert damit den Datenfluss. Neben der Verschiedenheit der Syntax liefern die meisten Datenquellen keinerlei semantische Informationen. Ist der Kontext der bearbeitenden Stellen in der Organisation ähnlich, entstehen wenige Probleme. Sobald der Kontext aber stärker ändert, z.B. eine andere Abteilung oder eine ausländische Sparte die Daten verarbeitet, dann führen Missverständnisse und Fehlinterpretationen zu vermehrten Problemen.

3.3 Bestehende Standards

Es stellt sich die Frage, inwieweit Frameworks, welche für ein Integrationskonzept geeignet sind, in der Literatur bereits beschrieben sind und wo noch Lücken bestehen. Um diese Frage zu beantworten, werden in 3.4 und 3.5 Konzepte vorgestellt. Diese werden in 5.3 evaluiert. Praktische Situationen werden auf der

Basis von Interviews in 4 empirisch belegt und thematisiert. Im folgenden sollen High Level Standards und technische Standards unterschieden werden. Unter High Level Standards werden CobIT, ITIL, ARIS sowie ISO17799, unter den technischen Standards werden XML und XBRL[31] untersucht. High Level Standards sind eher abstrakt in ihrer Formulierung und an keine Technologie gebunden. Technische Standards sind konkrete Technologien, welche die Anforderungen an eine Integration erfüllen könnten.

3.4 High Level Standards

Bestehende, etablierte High Level Standards sind mögliche Kandidaten für ein Integrationskonzept. Die folgenden Standards CobIT, ITIL, ARIS sowie ISO17799 sollen genauer betrachtet werden. Es ist später zu prüfen, inwieweit diese den Ansprüchen einer Integration von IT-Risikomanagement und IT-Controlling gerecht werden.

3.4.1 CobIT

3.4.1.1 Kurzbeschrieb

CobIT wurde Anfang 1996 mit dem Ziel entwickelt, allgemein anwendbare und allgemein akzeptierte Standrads (‚generally applicable and accepted') für IT-Security und IT-Controlling festzulegen. CobIT basiert auf den Kontrollzielen wie sie in den "Information Systems Audit and Control Foundation's (ISACF)"[32] definiert werden. Diese wurden erweitert mit internationalen technischen, regulatorischen und industriespezifischen Standards. In gewissen Bereichen erfolgt sogar eine terminologische (englische) Anpassung an die ‚Generally Accepted Accounting Principles (GAAP)'[33] des ‚Financial Accounting Standard Board (FASB)'[34]. Allgemein anwendbar und allgemein akzeptiert heisst, dass die vorliegenden Standards in einem Expertengremium abgestimmt wurden. Der CobIT Standard ist vom Umfang her eher bescheiden und versucht bereits etablierte Standards wie EDIFACT, ITSEC, ISO9000, CommonCriteria, COSO Report, IFAC, BS7799 oder ISO 17799 zu integrieren.

[31] Akronym für ‚Extended Business Reporting Language'
[32] [ISACF]
[33] [GAAP]
[34] [FASB]

3.4.1.2 Konstituierende Elemente

Der CobIT Standard konstituiert sich aus folgenden wichtigen Dokumenten:

- *Executive Summary*
  Gibt eine Übersicht über den Hintergrund und die Konzepte von CobIT
- *CobIT Framework*
  Definiert die Anforderungen an Informationen im Geschäftsumfeld. Daraus ergeben sich erste Kontrollziele auf hoher Abstraktionsstufe.
- *Control Objectives*
  Hier werden die 318 Kontrollziele der 34 Prozesse mit spezifischen Zielen beschrieben.
- *Audit Guidelines*
  Die Audit Guidelines dienen der Planung und Unterstützung der Auditaktivitäten
- *Management Guidelines*
  Die Management Guidelines helfen, den aktuellen Status der Unternehmung zu bestimmen. Dabei wird die Identifikation von kritischen Aktivitäten unterstützt, die Umsetzung gemessen, sowie die Zielerreichung festgestellt.

Wichtige Konzepte und Hilfsmittel sind dabei:

- *Domains & Processes*
  Eingeteilt in 4 Domains werden 34 Prozesse beschrieben.
- *Key Success Factors*
  KSF's geben Fähigkeiten an, die benötigt werden um die Ziele zu erreichen.
- *Key Goal Indicators*
  KGI's messen, ob die Ziele erreicht wurden.
- *Key Performance Indecators*
  KPI's messen den Fortschritt in Richtung Zielerreichung
- *Information Criteria*
  Die IC geben an, welche Kriterien Informationen erfüllen müssen, um dem Business zu genügen. Diese sind Effektivität, Effizienz, Vertraulichkeit, Integrität, Verfügbarkeit, Compliance sowie Verlässlichkeit.
- *Maturity Model*
  Das MM gibt darüber Auskunft, in welchem Zustand sich eine Unternehmung

hinsichtlich ihrer Prozesse befindet. Mögliche Stationen sind dabei ‚nicht existent', ‚initiiert', ‚teilweise definiert', ‚definiert', ‚kontrolliert' und ‚optimiert'.

CobIT unterscheidet verschiedene IT Ressourcen. Diese geben verschiedene Objekte eines Informationssystems wieder.

- *Daten*
  Alle Arten von Daten (Texte, Bilder, Audio...) in strukturierter oder unstrukturierter Form. Gemeint können Firmendaten oder externe Daten sein.
- *Anwendung*
  Alle Prozeduren, automatisiert, manuell oder eine Mischung davon.
- *Technologie*
  Beinhaltet Hardware, Software, Betriebssysteme, DBMS oder Netze.
- *Facilities*
  Die Gesamtheit von Ressourcen, welche Informationssysteme beherbergen und eine geeignete Betriebsumwelt gewährleisten.
- *Menschen*
  Die Fähigkeiten der Mitarbeiter, Informationssysteme zu planen, beschaffen, betreiben oder unterstützen.

Mit Hilfe der CobIT Dokumente, der Konzepte sowie der Hilfsmittel soll die IT einer Unternehmung kontrolliert und in sicheren Bahnen verlaufen.

Das CobIT Framework ist auf einem hohen Abstraktionsniveau angesiedelt, auch wenn konkrete Prozesse vorgegeben sind, explizit Vorschläge für KPI's etc. gemacht werden. Das Framework befasst sich nicht mit Problemen des Datenaustausches oder der Heterogenität der Systeme und bereits existierender Controllingprozessen.

3.4.1.3 Einbezug Risikomanagement

CobIT konzentriert sich auf das IT-Controlling sowie Sicherheitsfragen. Risikomanagement wird bewusst ausgeschlossen. Folgendes Zitat[35] aus den FAQ's macht das deutlich.

[35] [ISACA_RISK]

Die Frage lautete „Why are there not any Risk Statements with the Control Objectives?".

Die Antwort in gekürzter Form: „The provision of risk statements was seriously considered and investigated during the research and review phase of the initial COBIT project, but not retained because management preferred the pro-active approach (objects are to be achieved) over the reactive approach (risks are to be mitigated). The risk approach comes in at the end of the audit guidelines when the risk of not implementing the controls is substantiated. In the application of COBIT, the risk approach is certainly useful when management decides which controls to implement or when auditors decide which control objectives to review. Both of these decisions depend entirely on the risk environment".

Ein durchgehendes Risikomanagement wird also eher stiefmütterlich behandelt. Sicher sind Aspekte des Risikomanagements bereits in CobIT Prozessen enthalten, welche sich mit IT Sicherheit befassen. Einem IT-Risikomanagement im erweiterten Sinne wie unter 3.1 ausgeführt, entspricht das aber sicher nicht.

3.4.2 ITIL[36]

3.4.2.1 Kurzbeschrieb

ITIL, die "Information Technology Infrastructure Library", ist ein "Best Practice Framework" für die Definition und den Betrieb von IT-Prozessen. Träger dieser öffentlich zugänglichen Bibliothek ist das OGC, eine britische Regierungsbehörde, unter deren Regie ITIL gegen Ende der 80er Jahre entwickelt wurde. ITIL besteht derzeit aus einem Satz von ca. 40 Büchern, in denen die wichtigsten IT-Prozesse beschrieben werden. Der Umfang über 40 Bände hebt sich klar vom eher schlanken CobIT Standard ab. ITIL ist stark auf SLA Management ausgerichtet. ITIL liefert ein prozessorientiertes Vorgehensmodell, das sich auf die Erbringung und Einhaltung qualitativ hochwertiger IT-Dienstleistungen konzentriert. ITIL ist ein nicht proprietäres, öffentlich verfügbares Rahmenwerk unabhängig von Branche und IT-Technologie.

[36] In Anlehnung an [ITIL]

3.4.2.2 Konstituierende Elemente

ITIL basiert auf einem einheitlichen Prozessmodell und deckt 40 Themenbereiche ab. Diese Bereiche sind je in einem Band abgefasst. Die Aufzählung folgender Bereiche soll nur einen Ausschnitt wiedergeben:

- Incident Management
- Problem Management
- Configuration Management
- Change Management
- Release Management
- Service Level Management
- Availability Management
- Capacity Management
- IT Service Continuity Management
- Financial Management of IT Services
- Security Management
- Planning and Control for IT Services
- Quality Management for IT Services
- Computer Operations Management
- Network Services Management

3.4.2.3 Einbezug Risikomanagement

Gewisse Aspekte tangieren sicher Bereiche aus dem IT-Risikomanagement, allerdings weil dies eher zu einem funktionierenden IT-Service gehört. Zu nennen wären z.B. die Bereiche ‚Incident Management' oder ‚Problem Management'. Der durchgehende Ansatz eines Risikomanagements wie in 3.1 dargelegt, fehlt aber. Die Perspektive der damit verbundenen Gefahren oder Chancen für das Unternehmen steht nicht im Zentrum.

Weiter beinhaltet ITIL ein Prozessmodell, welches definiert was getan werden muss. ITIL hält sich jedoch sehr bedeckt, wenn es um Fragestellungen geht, wie die Prozesse in eine bestehende IT-Organisation eingeführt werden können. Diese Beschränkung des Frameworks sowie die knappe Behandlung des Risikomanagements sind nicht die besten Voraussetzungen für den hier zu diskutierenden integrativen Ansatz.

3.4.3 ARIS

Abbildung 9 illustriert das Zusammenspiel der wichtigsten Elemente des ARIS Frameworks. In folgenden drei Punkten soll ARIS kurz beschrieben werden.

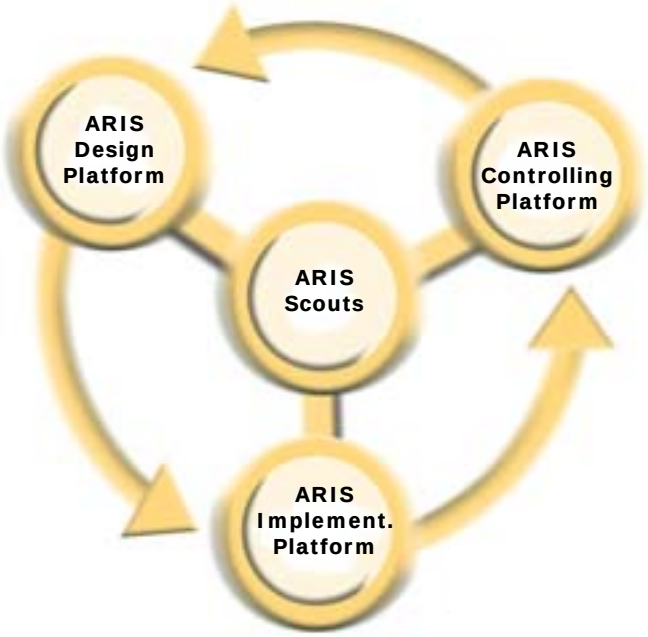

Abbildung 9: ARIS Framework

3.4.3.1 Kurzbeschrieb

ARIS wird von der Firma IDS[37] kommerziell vertrieben. ARIS bietet ein komplettes Portfolio für Entwicklung, Design, Implementierung, Betrieb, Controlling, Auswertung sowie die Optimierung von Geschäftsprozessen. Da sich IDS[38] nicht explizit an etablierte Standards anlehnt und nicht verspricht, auf diesen aufzubauen, sind die zugrunde liegenden Konzepte nicht transparent.

3.4.3.2 Konstituierende Elemente

ARIS ist in Plattformen organisiert. Siehe hierzu auch Abbildung 9 oben. Dabei werden folgende drei Hauptplattformen unterschieden:

- *ARIS Design Plattform*

  Die Design Plattform besteht unter anderem aus einem Modul für das WEB, dem Toolset, einer Simulationslösung, sowie einer Anwendungen für BSC[39]. Die Designplattform unterstützt dabei das dezentrale Prozessdesign.

[37] [IDS]
[38] [IDS]
[39] Akronym für ‚Balanced Scorecard'

- *ARIS Implementation Plattform*
  Die Implementation Plattform bietet Unterstützung bei der Umsetzung der designten Prozesse. Dabei werden Brücken zwischen spezifischen Produkten und Technologien geschlagen. So werden MySAP, CRM Systeme oder XML genannt.
- *ARIS Controlling Plattform*
  Die Controlling Plattform teilt sich in die Bereiche Prozesskostenanalyse und Prozess-Performanceanalyse auf.

Daneben erlauben die ARIS *Scouts* die Erweiterung von ARIS auf Themenbereiche wie:

- Qualitätsmanagement
- Prozessrisiken
- Neudokumentation
- Software Engeneering

Von speziellem Interesse sind hier der Scout für Prozessrisiken. Der ARIS Process Risk Scout ist ein Werkzeug für den Aufbau und operativen Betrieb eines Risikomanagementsystems. Auch ARIS interpretiert Risiko jedoch nur im Sinne einer Gefahr. Zitat[40]: „Um diese Risiken erkennen und effizient vermeiden zu können, muss jedes Unternehmen ein funktionierendes Risikomanagement aufbauen“.

3.4.3.3 Einbezug Risikomanagement

Die Controllingplattform sowie der Process Risk Scout kommen einer Integration von IT-Controlling und IT-Risikomanagement nahe. Es ist anzunehmen, dass ein vollständig implementiertes ARIS hohe Effizienzgewinne durch die so erzielte Integration realisieren kann. Ein Problem ist dabei die vollständige Prozessorientierung. Die meisten Firmen sind meilenweit von einer vollständigen Prozesskostenrechnung in der IT entfernt, diese ist höchstens teilweise vorhanden. Der partielle Einsatz von ARIS bringt aber die erwünschten Effizienzgewinne nicht mit sich. Eine verstärkte Integration von IT-Controlling und IT-Risikomanagement wäre nur zu erwarten, wenn ARIS breit eingesetzt würde.

[40] [IDS]

3.4.4 ISO 17799

3.4.4.1 Kurzbeschrieb

Im Jahr 1995 veröffentlichte das BSI[41] den ersten Sicherheitsstandard, BS 7799, der darauf ausgerichtet war, die Sicherheitsaspekte im Zusammenhang mit E-Commerce abzudecken. Seit der Einführung im Dezember 2000 hat sich der ISO 17799 zum weltweit am häufigsten anerkannten IT-Sicherheitsstandard entwickelt. Der aktuelle ISO 17799-Standard ist eine Sammlung von Empfehlungen für IT-Sicherheitsverfahren und -methoden, die sich in der Praxis bewährt haben (Best Practices). Die Norm dient als Basis für die Entwicklung unternehmensweiter Sicherheitsstandards für die IT. ISO 17799's Ziele sind die Identifikation, Steuerung sowie Minimierung von Risiken.

3.4.4.2 Konstituierende Elemente

ISO 17799 ist in 10 Sektionen organisiert. Diese sind:

- *Business Continuity Management*
  Fallen wichtige Informationssysteme aus oder treten Fehler auf, welche den ordungsgemässen Betrieb verunmöglichen, müssen Massnahmen und Pläne definiert sein, um den alternativen Betrieb oder den Systemwiederanlauf zu gewährleisten.
- *System Access Control*
  Wichtige Unternehmensdaten müssen vor unautorisiertem Zugriff geschützt werden. Neben den Daten an sich muss auch der Zugriff auf ganze Informationssysteme vor unautorisiertem Zugriff geschützt werden, dazu gehören Netzwerke, Desktopsysteme, Remotezugriff über Dial-in oder Terminals. Findet ein unautorisierter Zugriff dennoch statt, muss das registriert und aufgezeichnet werden.
- *System Development and Maintenance*
  Sicherheitsfunktionen müssen bereits bei der Systementwicklung integriert werden. Die Applikationen müssen so gestaltet werden, dass die Daten vor Verlust, Veränderung und Missbrauch geschützt sind. Projekte müssen so geführt werden, dass die sicherheitsrelevanten Belange voll berücksichtigt werden.

[41] [BSI]

- *Physical and Environmental Security*
  Unautorisierter Zugang zu Gebäuden und Räumen mit sicherheitskritischer Infrastruktur muss verhindert werden.
- *Compliance*
  Es muss sichergestellt sein, dass gesetzliche und regulatorische Vorschriften eingehalten werden. Weiter müssen interne Richtlinien eingehalten werden.
- *Personnel Security*
  Risiken welche von Mitarbeitern ausgehen sollen minimiert werden. Solche Risiken können Missbrauch oder Diebstahl von Daten oder anderen Informationsinfrastrukturen sein.
- *Security Organization*
  Sicherheitsbelange müssen auch in Fällen von Datenbearbeitungen durch dritte oder beim Outsourcing eingehalten werden. Zu jeder Zeit muss klar sein, wer welche Pflichten und Rechte in sicherheitskritischen Systemen hat.
- *Computer & Operations Management*
  Primärziel ist der richtige und sichere Betrieb der Informationsinfrastrukturen. Dies beinhaltet die Minimierung von Systemausfällen, der Schutz der Integrität der Daten oder die Gewährleistung von Integrität und Verfügbarkeit von Applikationen und Netzen.
- *Asset Classification and Control*
  Die Festlegung, welches System welchen Schutz benötigt und auch bekommt, ist essentiell für ein sinnvolles Sicherheitsmanagement. Dies muss durch entsprechende Kontrollen überwacht werden.
- *Security Policy*
  Die Security Policy gibt dem Management die entsprechenden Entscheidungsgrundlagen für sicherheitsspezifische Fragen.

ISO 17799 ist einer der meist verbreiteten Standards weltweit. Diese Aussage wird auch durch die geführten Interviews mehrfach gestützt.[42]

3.4.4.3 Einbezug Risikomanagement

ISO 17799 ist an sich ein Framework zur Beurteilung von Risiken. IT-Risikomanagement ist der tatsächliche Gegenstand von ISO 17799. Der Aspekt des IT-Controllings wird dagegen fast ausgeblendet. ISO 17799 interpretiert den Begriff

[42] [INTERVIEWTRANSKRIPTE]

Risiko auch vollständig als Gefahr. Die Interpretation von Risiken als Chance wird nicht miteinbezogen.

3.5 Technische Standards

Technische Standards bieten im Gegensatz zu High Level Standards zwei Vorteile. Erstens ermöglichen sie eine Koexistenz mit parallel angewandten High Level Standards, z.B. CobIT und ISO 17799. Ein technischer Standard kann sogar eine Brückenfunktion zwischen verschiednen High Level Standards wahrnehmen. Zweitens bieten technische Standards die Möglichkeit einer Durchsetzung mittels Codierung. Gemeint ist damit die später in 5.1 erläuterte Möglichkeit, der besseren Durchsetzung von Unternehmensweiten Regeln durch feste Programmierung von Abläufen. In den nächsten Kapiteln folgt eine Darstellung von XML und darauf aufbauend XBRL.

3.5.1 XML

XML, Extended Markup Language ist ein Standard zur Beschreibung von Daten. Nutzdaten werden in ihre Metainformationen eingebettet, welche einen Teil der Semantik der Daten wiedergeben. XML fokussiert vollständig auf die Daten und ihre Bedeutung, Aspekte der Darstellung und Struktur werden gesondert beschrieben. XML ist ein offizieller w3.org Standard seit 1998.

Datenaustauschformat

Klassische Datenbanksysteme (DBS) speichern Daten zentral ab und trennen Daten von Struktur und Darstellung. Diese Trennung von Daten, Darstellung und Struktur ist auch in XML vorhanden und macht XML für Datenbankanwendungen und Datenaustausch potentiell interessant. XML erfüllt nur den ersten Punkt nicht, die zentrale Speicherung der Daten. Die Entwicklung von XML-basierten DBS sind aber bereits in Entwicklung.

Trennung von Daten, Struktur und Darstellung

In XML sind Daten, Darstellung derselben sowie die Struktur von Daten getrennt. Ein XML File enthält nur die Daten, das XSD enthält die Struktur und das XSL die Darstellung.

Baumstruktur

Jedes XML Dokument lässt sich als Baum darstellen. Die Knoten werden durch die Elemente gebildet. Diese Eigenschaft macht sie für Datenbankanwendungen interessant und eröffnet die Möglichkeit, Bereiche im XML File über diese Struktur direkt zu addressieren.

Abgrenzung zu HTML

XML wurde zur Beschreibung von Daten entwickelt und konzentriert sich auf die Frage, was die Daten bedeuten. HTML wurde zur Darstellung von Daten entwickelt und konzentriert sich auf die Frage wie die Daten aussehen sollen. Die Darstellung von Daten kann in HTML programmiert werden, die Bedeutung ist in HTML fix definiert und kann nicht geändert werden. Auch die Struktur von Daten kann in HTML nicht definiert werden.

Einbettung in SGML Framework

XML ist wie HTML Teilmenge des SGML Standards und direkt aus SGML ableitbar. XML bietet die wichtigsten Vorteile von SGML, ist aber weniger komplex.

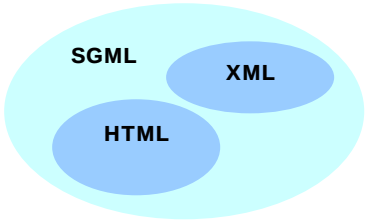

Abbildung 10: SGML, Obermenge von XML

3.5.1.1 Elemente von XML

XML (Extended Markup Language)

Das Hauptelement von XML ist das XML-File selbst, hier sind die Daten enthalten. Alle weiteren Elemente fügen sich der Syntax von XML. Unten folgen die wichtigsten Regeln der XML Syntax. Jedes XML Dokument enthält die Angabe um welche Version es sich handelt und welche Zeichencodierung angewandt werden soll.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

Weiter enthält jedes XML Dokument genau ein Root Element, welches bezeichnet um was für ein XML Dokument es sich handelt, z.B. eine Notiz.

<note>

Dann folgt ein Ansammlung von hierarchischen, dem Rootelement untergeordneten Elementen. Jedes dieser Elemente muss mit einem Starttag beginnen und mit einem Closingtag enden. Die Verschachtelung ist relevant. Daten können sowohl in Tags als Content

<note id>823</note id>

als auch in Form von Attributen

<note id="823">

angegeben werden. Prinzipiell sind Attribut und Taged Data austauschbare Darstellungsformen. XML Dokumente sind well formed, wenn sie den syntaktischen Regeln entsprechen.

XSL (Extendeted Stylesheet Language)

Erscheinungsbild

Hier geht es um die Definition des Erscheinungsbildes der Daten. Die Syntax entspricht der oben ausgeführten allgemeinen XML Syntax. Hier wird für jedes Element angegeben, wie die Daten im XML Dokument dargestellt werden sollen. Da das XSL File selber wieder ein XML file ist, kann leicht Konfusion aufkommen. Es sind zwar alles XML Files, aber die Rolle der Files ist unterschiedlich. Diese Rolle ist aus dem XML File ersichtlich, ein XSL File enthält als Rootelement ‚Stylesheet'.

Verknüpfung von XML und XSL File

Bei der Verknüpfung von XML und XSL File werden die Elementbezeichner der Ursprungsdaten selbst zu Daten im XSL File. Die Elementbetzeichner im XSL richten sich an die darstellende Software, die weiss was sie bedeuten. Z.B. bedeutend für Internet Explorer 6 <h2>...<\h2> dass es sich um einen Titel handelt, welcher gemäss den Einstellungen anzuzeigen ist. Die Tags im XSL File haben für die Maschine Bedeutung, nicht aber die dargestellten Daten.

Da meistens eine Darstellung in einem Browser gefragt ist, wird ein Stylesheet verwendet, welches dem Namespace des HTML Standards folgt. Das heisst, dass alle Tags gleich gedeutet und damit dargestellt werden.

Stylesheetvarianten und Namespaces

Es sind unterschiedlichste Stylesheets mit demselben Namespace möglich. Je nach Anforderungen können die Daten entsprechend dargestellt werden, jedoch immer innerhalb des Namespaces. Stylesheets können aber auch auf komplett anderen Namespaces aufbauen. Sollen die Daten nicht von einem HTML 4.0 Browser dargestellt werden, sondern von einem HTML 1.0 Browser, so kann der entsprechend ältere Namespace gewählt werden. Auch selber definierte Namespaces sind möglich.

Mit XSL verbundene Standards

Eng mit XSL verbunden sind die Standards XSLT, XPath sowie XSL Formating Objects. XSLT als wichtigster Teil von XSL beschäftigt sich mit der Transformation von XML in XHTML unter Anwendung von XSL. Als Element von XSLT ermöglicht XPath die Definition von Bereichen in XML Dokumenten. Die geschieht durch direkte Adressierung der Knoten in einem XML File. XSL Formating Objects spezifiziert die Outputformatierung bei einer Transformation von XML in XHTML unter Anwendung von XSLT.

DTD (Document Type Definition)

Gemäss den Syntaktischen Regeln von XML lassen sich unzählige Dokumente erzeugen. Mit DTD lassen sich die zulässigen Dokumente einschränken. DTD definieren, welche Datenstruktur XML Dokumente haben müssen. Konkret geben DTD grob an, welche Elemente vorhanden sein müssen und wie diese verschachtelt sind. Eine DTD kann direkt in einem XML File enthalten sein, oder als separates Files definiert werden. DTD sind verbreitet, aber eher veraltet. An Stelle von DTD's treten vermehrt XML Schemas.

XSD (XML Schema definition)

Wie DTD's beschreiben XML Schemas die Struktur von XML Dokumenten, welche Elemente vorhanden sein müssen und wie diese verschachtelt sind. Auch XML Schemas sind in XML Syntax verfasst. Schemas erlauben im Gegensatz zu DTD's die

Spezifizierung von Datentypen. Dies erleichtert den Einsatz in Datenbankanwendungen. Durch die genauere und damit bessere Spezifizierbarkeit, wie Daten auszusehen haben, wird auch die Interoperabilität mit andern Systemen vereinfacht. Werden XML Files ausgetauscht, so ist nun klarer wie die Daten auszusehen haben. Weniger Fehler entstehen. Werden Schemas eingesetzt, so reicht das Kriterium ‚well formed' nicht mehr aus, um ein valides XML vor sich zu haben. Das XML File muss auch noch den Anforderungen des Schemas genügen. Schemas lassen sich daher zur Beschreibung und Einhaltung eines Datenmodells heranziehen. Diese Eigenschaft von Schemas erinnert an die Schemadefinition einer herkömmlichen Datenbank.

Ein Schema wird durch folgende Tags eingeleitet und beendet:

<schema>.....</schema>

Namespaces

Namespaces helfen, Konflikte bei der Namensgebung von Elementen in XML Dokumenten zu verhindern. Es geht nicht um eine globale Definition von Namen, welche die gleiche Bedeutung haben, vielmehr geht es um die Zuordnung eines Namens zum entsprechenden Kontext. Elementbezeichnungen werden Präfixe vorangestellt, welche Namen eindeutig machten.

<x:note xmlns:x="http://www.danielschmid.com/note">

Der spezifizierte Namespace sollte gemäss W3C immer ein Uniform Ressource Identifier (URI) sein. Domainnamen eignen sich dazu besonders gut, sind diese doch weltweit eindeutig.

Die Angabe des Namespaces *"http://www.danielschmid.com/note">* impliziert nicht, dass unter dieser Addresse ein Dokument existiert, welches abgerufen werden könnte. Es bedeutet lediglich, dass jemand den Anspruch auf Eindeutigkeit eines Namespaces erhebt. Diese Instanz kontrolliert die URL. Aber im Prinzip könnte jeder irgend einen Namespace spezifizieren, ohne dazu berechtigt zu sein.

3.5.2 XBRL

Definition

„XBRL ist eine frei verfügbare elektronische Sprache für das "Financial Reporting", also den Austausch von Informationen von und über Unternehmen, insbesondere von Jahresabschlüssen. XBRL bietet einen Standard für die Erstellung, die Verbreitung/Veröffentlichung, Auswertung und den Vergleich solcher Informationen.“ [43] XBRL basiert auf XML. XBRL ist XML, welches mit einem definierten XML-Schema angewandt wird. Die Schemadefinitionen werden in XBRL Taxonomien genannt.

Abgrenzung zu Microsofts OLE Schnittstelle

XBRL ist ein semantischer Standard, nicht wie Microsofts OLE Schnittstellen, welche nur die syntaktische Ebene abdecken. XBRL definiert in Taxonomien vorkommende Begriffe exakt.

Taxonomien

Die Struktur der Daten ist in XBRL in einer Taxonomie definiert. Diese Taxonomie ist in verschiedene Files aufgeteilt, einerseits XML Schema Files (.XSD) als auch XML Files (.XML). Die Taxonomie definiert die verschiedenen Elemente, aus welchen ein XML Informationspaket besteht. Ein Informationspaket ist eine Reportingeinheit, z.B. eine Unternehmung über eine bestimmte Periode.

Wichtigste Bestandteile von Taxonomien sind die Elemente mit ihrer Referenz (z.B. ISA-Text oder Gesetze) sowie Formatdefinitionen und Beziehungen der Elemente untereinander. So enthält zum Beispiel die deutsche XBRL Taxonomie die folgenden, zentralen Elemente:

- german_ap.xsd: Elementdefinitionen
- german_ap_calculation.xml: Calculation linkbase
- german_ap_label.xml: Label linkbase
- german_ap_definition.xml: Definition linkbase
- german_ap_presentation.xml: Presentation linkbase
- german_ap_reference.xml: Reference linkbase

[43] [XBRL_DEUTSCHLAND]

Jedes Land muss entsprechend den nationalen Gepflogenheiten eine eigene Taxonomie erstellen. Die Existenz von nationalen Taxonomien ist daher auch stark davon abhängig, ob eine nationale ‚Group of Interest' existiert. Für verschiedene Länder wie z.B. Deutschland, Neuseeland, USA, Singapur oder Spanien bestehen solche Gruppen. Auch internationale Taxonomien, losgelöst von nationalen Bestimmungen, für IAS und USGAAP liegen vor. Im Mai 2002 wurde auch eine Arbeitsgruppe zu BASEL II eingerichtet[44]. Damit dürfte auch das Risikomanagement in einem erweiterten Rahmen Einzug in XBRL halten.

Bei der Erstellung der entsprechenden Taxonomien ist viel Fachwissen über lokale und internationale Reportingbestimmungen nötig. Taxonomien enthalten im Falle der deutschen Taxonomie ca. 1300 Positionen, welche in folgende Bereiche gegliedert sind:

- Allgemeine Informationen
- Bilanz
- Gewinn- und Verlustrechung
- Gewinnverwendung / Eigenkapitalspiegel
- Kapitalflussrechnung
- Anhang, Lagebericht

3.5.2.1 Einsatz

XBRL erlaubt es dem Unternehmen, ihre Daten nur einmal aufzubereiten um sie dann in den verschiedensten Formen zu veröffentlichen. Auch spezielle Informationspflichten, z.B. für die Börsenaufsicht, die Bankenkommission, Handelsregister oder Versicherungsanstalten. Auch für das externe Reporting zu Händen der Shareholder oder anderen Stakeholdern können die Daten in entsprechender Form zur Verfügung gestellt werden. XBRL schränkt das Unternehmen weder in der Wahl von Rechnungslegungsverfahren ein, noch muss es Informationen preisgeben, welche es vorher nicht veröffentlichen wollte.

Abbildung 11 zeigt schematisch die groben Zusammenhänge einer XBRL Architektur. Pfeile versinnbildlichen dabei Datenflüsse. Die verschiedenen Bereiche des internen Reportings kommunizieren dabei in einer mehr oder weniger unstrukturierten

[44] [XBRL_DEUTSCHLAND]

Weise. Auch die Datenlieferungen aus den Vorsystemen erfolgen dabei in heterogenen Datenformaten und diversen Tools. Nicht nur die Datenformate sind verschieden, auch die Bedeutung der gelieferten Daten liegt ohne zusätzlichen Abgleich mit den zuständigen Stellen oft im Dunkeln.

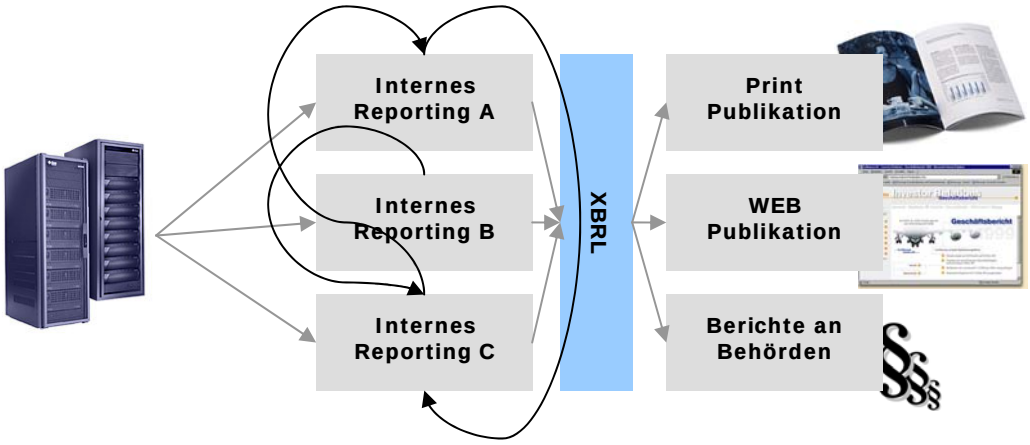

Abbildung 11: XBRL Architektur

Instanzdokumente

Instanzdokumente sind XML Fragmente mit einem XBRL Rootelement. Sie enthalten die konkrete Reportinginformation, z.B. ein über das Internet veröffentlichter Geschäftsbericht. Die zugrundeliegende Taxonomie bestimmt dabei die zulässige Struktur oder die Datenformate von Elementen im Instanzdokument.

Praktisches Vorgehen

Soll ein Report im XBRL Format erstellt werden, müssen folgende Schritte durchlaufen werden[45]:

- Daten generieren
  (z.B. Bezug aus Datenbanken oder Transaktionssystemen)
- Bestimmung der anzuwendenden Taxonomie
  (z.B. IAS Taxonomie, oder Erzeugung einer neuen)
- Zuordnung der Daten zur Taxonomie
  (z.B. Abgleich der Begriffe der internen Buchhaltung mit denjenigen von IAS)
- Erzeugung des Instanzdokuments

[45] [XBRL_NEWZEALAND]

Der einfachste Weg besteht darin, dass der Softwarehersteller eine XBRL Schnittstelle fest einbaut und somit das XBRL Schema fest einbaut. Dies ermöglicht die automatische Zuordnung. Allerdings verliert man so an Flexibilität, welche gerade beim internen Reporting unbedingt nötig ist.

XBRL für das interne Reporting

Wollen Unternehmen XBRL auch für interne Berichtswege verwenden, so steht es ihnen frei, mit einer erweiterten Taxonomie zu arbeiten. Je nach gewünschtem Detaillierungsgrad müssen zusätzliche Elemente definiert werden. Im Idealfall kann das interne Reporting wie das externe aus den gleichen Datenbeständen generiert werden. Solche zusätzlichen unternehmensspezifischen Elemente müssen aber von den Unternehmen selber erstellt werden. Zum Zeitpunkt der Erstellung der vorliegenden Arbeit waren keine fertigen Taxonomien für das interne Reporting bekannt.

3.6 Problembereiche einer Integration

Soll ein Integrationsmodell für IT-Controlling und IT-Risikomanagement gefunden werden, so haben spezielle Themenbereiche einen starken Einfluss auf den Erfolg der Integration. Diese Problembereiche sollen im folgenden genauer beleuchtet werden. Die Probleme gliedern sich in acht Teilbereiche:

- Organisation
- Mitarbeiter
- Infrastruktur
- Daten
- Tools
- Dynamik
- Komplexität
- Wirtschaftlichkeit

Eine Trennung der Gebiete ist nicht möglich, interagieren doch alle mehr oder weniger stark miteinander. Die folgenden Kapitel gehen nun genauer auf die einzelnen Punkte ein.

3.6.1 Organisation

Probleme im Bereich Organisation lassen sich grob in die Teilbereiche Organisationsform, Organisationsgrösse sowie Unternehmenskultur aufteilen.

3.6.1.1 Organisationsform

Unternehmen können auf unterschiedliche Art organisiert sein. Die beiden Extremformen bilden zentralistisch organisierte Unternehmen und solche, welche dezentral geführt werden. Dazwischen liegen Profit Center Organisationen oder Cost Center Organisationen. Je zentralistischer eine Unternehmung geführt wird, desto einfacher ist eine organisationsweite Einführung von einheitlichen Vorgehensweisen, wie die Integration von IT-Controlling und Risikomanagement. Sind Organisationen dezentral organisiert, haben die Teilbereiche entsprechend grössere Entscheidungskompetenzen. Diese erschweren eine konsistente Einführung von unternehmensweiten Konzepten. Hier basiert eine Konzeptdurchsetzung mehr auf Überzeugung und Konsens als im zentralen Fall. Zentral organisierte Firmen verordnen neue Konzepte und überwachen deren Umsetzung. Das eine ist nicht besser als das andere. Die Durchsetzung eines integrativen Konzeptes für IT-Controlling und Risikomanagement musss aber entsprechend angepasst durchgeführt werden. Eine zentrale Organisationsform erlaubt eine Top-Down Einführung. Eine dezentrale Organisation verlangt nach einer Kombination aus Top-down und Bottom-up Einführung.

3.6.1.2 Organisationsgrösse

Die Grösse einer Unternehmung hat sowohl grossen Einfluss auf die Art und Weise wie ein Integrationskonzept eingeführt wird, als auf die Art des Konzeptes welches angewandt werden soll. Bei kleineren Organisationen kann durchaus die gesamte Unternehmung auf einmal auf das neue Konzept umstellen. Bei grösseren Unternehmen ist ein schrittweises Vorgehen sinnvoll.

3.6.1.3 Unternehmenskultur

Je nach Branchezugehörigkeit und damit verbundenen kulturellen Unterschieden wird ein anderer Integrationsansatz gewählt. Ist die Kultur eher innovativ, nimmt die Organisation Änderungen leichter auf. Ist dagegen die Kultur eher auf Effizienz ausgerichtet, werden Änderungen eher träge aufgenommen. Wird der kulturelle

Kontext einer Unternehmung berücksichtigt, fällt die Einführung eines integrativen Konzeptes für IT-Controlling und Risikomanagement leichter.

3.6.2 Mitarbeiter

Jede Änderung führt zu personellen Wiederständen. Diese können je nach Interessenlage sehr stark sein. Da sie Interessenlage nicht immer klar ist, ist die Struktur der Wiederstände oft nicht transparent. Dies erschwert auch die Einführung eines Integrationskonzeptes für IT-Controlling und IT-Risikomanagement. Es ist sogar davon auszugehen, dass diese Schwierigkeiten hier besonders ausgeprägt sein werden, sind doch Kontroll-Informationen involviert. Soll ein Integrationskonzept für IT-Controlling und IT-Risikomanagement eingeführt werden, müssen diese Aspekte besonders berücksichtigt werden.

3.6.3 Infrastruktur

Infrastrukturen sind potentiell träge, lassen sich aber inkrementell anpassen. Komplette Systemwechsel sind sehr schwer zu erreichen. Konkret ist es einfacher auf bestehenden Infrastrukturen aufzubauen, als Systeme durch neue zu ersetzen. Allerdings lassen sich mit Neusystemen mehr sinnvolle Funktionen realisieren. Es besteht hier ein typischer Trade-off zwischen wünschbarer Funktionalität und Aufwand durch den Ersatz von Altsystemen.

Hat eine etablierte Anwendung zum Beispiel keine XML-Schnittstelle, so muss entweder auf eine neue Applikation umgestellt werden die das unterstützt, oder die Applikation muss angepasst werden. Die einfachste Lösung wäre der Einsatz einer Middleware, welche das Problem löst, ohne die Anwendung zu verändern. Welche Variante die sinnvollste ist, muss im Einzelfall geprüft werden, unter Abwägung von Kosten und Nutzen. Kosten und Nutzen müssen dabei nicht nur direkte Kosten sein. Auch Störungen von etablierten und produktiven Abläufen sind Kosten.

3.6.4 Daten[46]

Datenspezifische Probleme sind am vielschichtigsten, berühren die Daten doch alle anderen Bereiche. Die Probleme lassen sich in folgende Bereiche einteilen.

- Verfügbarkeit von Daten
- Richtigkeit der Daten

[46] In Anlehnung an das [COBIT] Framework

- Wirtschaftlichkeit der Datenbereitstellung
- Vertraulichkeitsprobleme
- Vollständigkeit der Daten
- Regulatorische Einschränkungen
- Einbezug externer Daten
- Konsistenter Einsatz des Integrationsframeworks
- Unterschiedliche Semantik
- individuelle Einschätzungen über die Relevanz von Daten
- Qualität von Daten

3.6.4.1 Verfügbarkeit von Daten

Daten können nicht verfügbar sein, weil sie intern nicht vorhanden sind. Oft sind relevante Daten im Unternehmen jedoch vorhanden, sind aber trotzdem nicht verfügbar. Die Gründe lassen sich in folgende Bereiche aufteilen:

Technische Gründe

Daten lassen sie sich nicht wie gewünscht aus Systemen extrahieren. Das kann am kompletten Fehlen von Schnittstellen liegen, oder die zur Verfügung stehenden Schnittstellen sind nicht geeignet. Oft stellen sich auch Versionsprobleme. Im Prinzip liessen sich entsprechende Schnittstellen einfach implementieren oder zukaufen. Dies ist aber mit Entwicklungsaufwand oder zusätzlichem Lizenzaufwand verbunden. Wird dieser z.B. aufgrund von gesteigertem Kostendruck nicht in Kauf genommen, fehlen eben geeignete Schnittstellen und als Folge daraus sind die Daten nicht verfügbar.

Personelle Gründe

Personelle Wiederstände spielen beim internen Datenaustausch in zunehmendem Masse eine Rolle. Aus Daten lässt sich Wissen extrahieren und Wissen ist bekanntlich Macht. Oft verbergen sich hinter technischen oder zeitlichen Gründen personelle Wiederstände. Beim Austausch von Daten sind daher immer eventuell bestehende personelle Wiederstände zu berücksichtigen. Neben Wiederständen kann auch mangelndes Know-how in der Bedienung der eingesetzten Tools Ursache sein. Als Folge daraus sind die Daten nicht verfügbar.

Zeitliche Gründe

Daten verlieren erfahrungsgemäss mit fortschreitender Zeit an Wert. Sollen sinnvolle Informationen aus Daten gewonnen werden, ist man meistens an aktuellen Daten interessiert. Je nach Auslastung der betroffenen Ressourcen, seien dies Menschen oder Systeme, können Daten möglicherweise nicht schnell genug geliefert werden. Folglich sind die Daten nicht verfügbar.

3.6.4.2 Richtigkeit der Daten

Wenn nicht genau klar ist, welche Daten aus welchem System mit welchen Parametern extrahiert werden soll, so können Missverständnisse auftreten. Auf die Anforderung, die Gehaltszahlen ‚aller Mitarbeiter' zur Verfügung zu stellen, stellt sich die Frage, was genau unter Mitarbeitern verstanden wird. Sind das nur Mitarbeiter in einem regulären Vertragsverhältnis oder ist dabei möglicherweise auch eingemietetes Personal eingeschlossen? Oft werden solche Inkongruenzen erst spät bemerkt und mindern die Qualität der gewonnen Informationen. Oft muss die Arbeit nochmals wiederholt werden, mit entsprechend angepassten Daten.

3.6.4.3 Wirtschaftlichkeit der Datenbereitstellung

Jede zur Verfügung Stellung von Daten kostet. Die schwierige Frage lautet, ob der erwartete Nutzen diese Kosten übersteigt. Die Beantwortung der Frage kostet selbst wieder. Ein praktikabler Ansatz ist, die Kosten der zur Verfügung Stellung der Daten zu minimieren. Dann ist zwar nicht sichergestellt, dass es wirtschaftlich ist, aber immerhin wird die Anzahl wirtschaftlicher Datenbereitstellungen erhöht.

3.6.4.4 Vertraulichkeitsprobleme

Enthalten Daten schützenswerte Informationen, so sind entsprechende Massnahmen zu treffen, dass diese Daten nicht von jedermann eingesehen werden können. Auch muss sichergestellt werden, dass die Daten nicht in schädlicher Weise weiterverbreitet werden. Schützenswert können personenbezogene Daten, z.B. einer Versicherungsgesellschaft oder Geschäftsbezogene Daten sein, z.B. Umsatzzahlen.

3.6.4.5 Vollständigkeit der Daten

Die Ursachen für unvollständige Daten sind vielschichtig. Fehlende Daten aufgrund von nicht vorhanden sein ist eine Ursache, unvollständige Daten durch Fehlmanipulationen an Systemen ist ein anderer. Werden z.B. Daten in mehreren Einzelschritten zu unterschiedlichen Zeitpunkten mit verschiedenen Parametern gewonnen, so ist die Vollständigkeit schwer zu überprüfen.

3.6.4.6 Regulatorische Einschränkungen

Handelt es sich bei den interessierenden Daten z.B. um schützeswerte, personenbezogene Daten, so untersagen Gesetze gewisse Verschiebungen genau dieser Daten. So ist es z.B. nicht erlaubt, geschützte, personenbezogene Daten ohne spezielle Massnahmen ins Ausland zu verschieben, z.B. um die Daten dort im Inland untersagter Manipulationen zu unterziehen. Eine solche heikle Verschiebung von Daten liegt schneller vor als vermutet. So kann das blosse speichern in einer ausländischen Serverfarm bereits zu Problemen führen.

3.6.4.7 Einbezug externer Daten

Die meisten Daten für das Controlling liegen intern vor, beschäftigt sich das Controlling doch primär mit den internen Abläufen. Bei Aufgaben wie dem IT-Risikomanagement oder bei Benchmarking müssen aber möglicherweise externe Daten beschafft werden, z.B. Benchmarkwerte. Alle Schwierigkeiten treten bei externen Quellen in verstärktem Masse auf, meistens ist die Beschaffung mit direkten, zusätzlichen Kosten verbunden.

3.6.4.8 Konsistenter Einsatz des Integrationsframeworks

Sollen Barrieren beim Austausch von Daten minimiert werden und wird dazu ein geeignetes Integrationsframework eingesetzt, so muss dieses Framework konsistent und nachvollziehbar eingesetzt werden. Es müssen alle beteiligten die gleiche ‚Sprache' sprechen. Wird das Framework nur partiell eingesetzt, so stiftet es nur Verwirrung, weil möglicherweise zusätzliche Datenformate und Begriffsontologien generiert werden.

3.6.4.9 Unterschiedliche Semantik

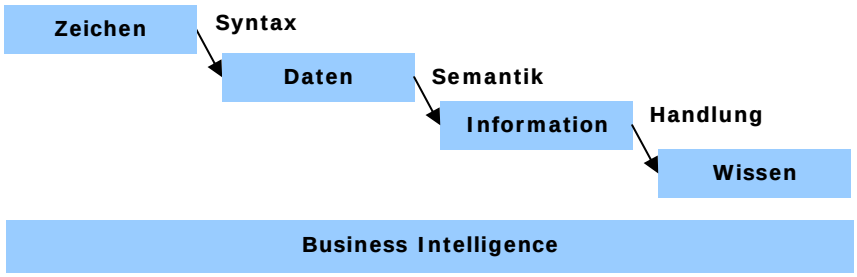

Abbildung 12: Vom Zeichen zum Wissen

Gemäss Abbildung 12 enthalten Files vorerst nur eine Ansammlung von Zeichen, entstammend einem technischen Standard welcher die zulässigen Zeichen erlaubt. Werden die Zeichen nun nach einer bestimmten Struktur, der Syntax angeordnet, so entstehen Daten. Weder mit einzelnen Zeichen noch mit den strukturierten Daten können wir viel anfangen. Möglicherweise entnehmen wir Daten bereits gewisse Informationen, dies aber nur, weil wir implizit eine Semantik zugrunde legen. So hat das Datum ‚25.04.03' möglicherweise die Bedeutung eines Kalenderdatums, einfach weil wir Kalenderdaten oft so schreiben und es implizit eine Konvention gibt, dass man Kalenderdaten so schreiben kann. Das Datum ‚25.04.03' kann aber auch eine völlig andere Bedeutung haben, so kann es auch eine Artikelnummer sein.
Kurz: Der Struktur von Daten entnehmen wir meistens auch ihre Bedeutung. Fehler treten dabei regelmässig auf. Gerade im Businessalltag können Missverständnisse auftreten, wenn die Begriffe nicht scharf oder neu sind. Abhilfe bietet meistens die Rückfrage und die Diskussion mit Kollegen. Sollen Datentransfers aber zwischen Maschinen stattfinden, so muss auch die Bedeutung von Daten explizit gemacht werden. Dies geschieht mit einer spezifischen Semantik. Jedem Datum wird ein Attribut zugeordnet, welches über seine Bedeutung Aufschluss gibt. Sind die Attribute gleich, haben zwei Daten die gleiche Bedeutung. <Datum>25.04.03<Datum\> hat immer die Bedeutung eines Kalenderdatums. <Artikelnummer>25.04.03<Artikelnummer\> die Bedeutung einer Artikelnummer.
Bei so einfachen Dingen wie Kalenderdaten und Artikelnummer ist die Bedeutung klar. Kompliziertere, weniger gebräuchliche Begriffen müssen entsprechend genau definiert werden. Es ist daher sinnvoll sich Organisationsweit auf eine kongruente Begriffsdefinition zu einigen. Diese Standardisierung ist ein Teil der Business Intelligence[47].

3.6.4.10 Individuelle Einschätzungen über die Relevanz von Daten

Gerade im Risikomanagement können die Einschätzungen über die Relevanz von Daten sehr unterschiedlich sein, auch wenn über die Bedeutung Einigkeit herrscht. Je nach Kontextinformationen die jeder Benutzer von Daten hat, enthalten diese unterschiedliches Wissen. Dies kann bei der Aggregation von Risiken zum Problem werden. Die individuellen Risikoeinschätzungen sind nach der Einschätzung meistens nicht mehr transparent, die Aggregation ist es erst recht nicht mehr.

[47] Business Intelligence ist eine Sammlung von Technologien und Anwendungen zwecks Sammlung, Speicherung, Zugriff und Analyse von Daten mit dem Zweck, bessere Entscheidungen zu treffen. Typische Anwendungen sind OLAP Anwendungen, Data Mining oder Statistiken.

Das Problem besteht auch bei klassischen Controllingaufgaben. Hier ist die Selektion und Ausblendung von Daten nach dem Entscheid nicht mehr transparent. Auch diese Entscheidung hat damit zu tun, welches Wissen jeder Anwender den Daten entnimmt, je nach seinem persönlichen Kontext.

3.6.4.11 Qualität von Daten

Eines der wichtigsten Probleme ist die Qualität der Daten. Frei nach dem GIGO Konzept lassen sich nur aus qualitativ hochwertigen Daten wertvolle Informationen und relevantes Wissen ableiten.

Qualität bedeutend, dass man das bekommt was man wollte. Nicht mehr und nicht weniger. Ist eine hohe Datenqualität verlangt, so darf der Anteil von Falschbuchungen oder der Anteil von nicht vollständig erfassten Datensätzen ein vorbestimmtes Mass (Qualitätslevel) nicht unterschreiten. Nach dem Wirtschaftlichkeitsprinzip sollte es das Mass auch nicht grob übersteigen, so dass der Aufwand, diese Qualität zu erzeugen im Vergleich zum Mehrnutzen der höherwertigen Daten wirtschaftlich nicht zu rechtfertigen wäre.

Die Qualität von Daten ist oft schwierig zu beurteilen. Dies hat damit zu tun, dass die Überprüfung gewisser Sachverhalte sehr aufwändig oder sogar unmöglich ist, ein Beispiel sind falsche Datenwerte. In einem solchen Fall muss von Annahmen oder von Stichproben ausgegangen werden.

3.6.5 Tools

Schreibt das Integrationskonzept keine speziellen Tools vor, so ist der Abstimmungsaufwand entsprechend höher. Jedes Tool hat bekanntlich seine Eigenheiten. Der konsistente Einsatz eines Integrationsframeworks erzwingt keine einheitlichen Tools, es ist aber wünschenswert, da effizienzsteigernd. So ist zum Beispiel denkbar, dass eine Abteilung Excel verwendet, eine andere aber Lotus 123[48]. Prinzipiell entstehen damit keine Probleme, allerdings ist erfahrungsgemäss ein höherer Aufwand für Konvertierungen erforderlich.

3.6.6 Dynamik

3.6.6.1 Wechselnde Anforderungen

Aufgrund von organisatorischen Änderungen, neuen regulatorischen Bestimmungen oder neuen Produkten und veränderten Märkten ändern sich die Anforderungen an

[48] Verbreitet in Firmen die historisch gewachsen Lotus Produkte eingesetzt haben, heute aber auf Microsoft umstellen.

eine Integration von IT-Controlling und IT-Risikomanagement. Dies deshalb, weil sich auch die Anforderungen an das Controlling und an das Risikomanagement geändert haben. Wird zum Beispiel ein Unternehmen gekauft, kommen neue Systeme, Produkte und Organisationseinheiten hinzu.

3.6.6.2 Organisation

Ändert sich die Organisation, so ändern sich auch die Strukturen mit denen sich das Controlling beschäftigt. Risiken müssen neu erkannt werden. Dies stellt hohe Anforderungen an ein Integrationskonzept.

3.6.6.3 Regulatoren

Ändern sich regulatorische Rahmenbedingungen, so wechseln automatisch auch die Bedingungen für das IT-Controlling und das IT-Risikomanagement. Dies hat Einfluss auf ein Integrationskonzept. Werden neue Richtlinien im Bereich Datenschutz erlassen, so ist das Controlling unmittelbar betroffen. Gewisse Daten dürfen möglicherweise nicht mehr ohne weiteres beliebig transferiert werden. Werden neue Gesetze zum Risikomanagement erlassen, wie z.B. das KonTraG[49] in Deutschland, so ändern sich die Anforderungen an das Risikomanagement.

3.6.6.4 Produkte & Märkte

Werden neue Produkte eingeführt, alte zurückgezogen oder verändern sich die Märkte, so ändern sich auch die Anforderungen an das IT-Controlling und das Risikomanagement. Diese hat Einfluss auf ein Integrationskonzept. Eröffnet ein Unternehmen zum Beispiel ein neues Rechenzentrum um neue Dienste anbieten zu können, so erweitern sich die Anforderungen an das IT-Controlling schlagartig. Auch die Risikolage hat sich dann verändert.

3.6.7 Komplexität

Komplexität steht dem Bedürfnis nach Transparenz entgegen. Die Schaffung von Transparenz ist aber eine der zentralen Aufgaben des Controlling und zum Teil auch des Risikomanagements. Die Herausforderungen an IT-Controlling und Risikomanagement sind bei komplexen Sachverhalten entsprechend hoch. Höher werden entsprechend die Anforderungen an ein Integrationskonzept. So ergeben sich

[49] Seit 1. Mai 1998 gelten für alle deutschen Kapitalgesellschaften, Börsen und amtlich notierten Aktiengesellschaften zahlreiche Vorschriften zur besseren Kontrolle und Transparenz im Unternehmen. Dazu gehört die Implementierung eines systematischen Risikomanagements.

zum Beispiel aus dem komplexen Sachverhalt von interdependenten Risiken zwischen Projekten auch hohe Anforderungen an das Integrationskonzept.

3.6.8 Wirtschaftlichkeit

Obgleich die Wirtschaftlichkeit hier an letzter Stelle aufgeführt wird, handelt es sich um den wichtigsten Punkt. Alle oben genannten Problembereiche münden zuletzt in der Wirtschaftlichkeit. Ist eine Massnahme zur Integration von IT-Controlling und IT-Risikomanagement nicht wirtschaftlich, so muss sie erst gar nicht in Betracht gezogen werden. Die Schwierigkeit liegt dabei allerdings bei der Bestimmbarkeit der Wirtschaftlichkeit. Zuletzt sind Massnahmen zur Integration nur wirtschaftlich, wenn entweder Erträge verbessert, die Qualität erhöht oder Kosten eingespart werden können. Dies kann in Form einer Reduktion des Personalbestandes oder der Systemkosten wie Lizenzen oder Hardware erreicht werden.

4 Interviews

Auf qualitativer Basis wurden persönliche Interviews in sechs Unternehmen geführt. Die Interviews wurden aufgrund eines Fragekatalogs strukturiert.

4.1 Ziele der Interviews

Die Interviews sollen Aufschluss darüber geben, welche praktischen Lösungsansätze für eine Integration von IT-Controlling und IT-Risikomanagement in Unternehmen bestehen. Diese Lösungen sollen in bestehenden internen Strukturen wie Richtlinien, praktischen Vorgehensweisen, Applikationen etc. gesucht werden.
Die so gewonnenen Informationen flossen in die Strukturierung der Arbeit sowie in die spätere Formulierung von Lösungsansätzen ein.

4.2 Festlegung der Interviewfragen

Die folgenden Fragen wurden den Interviewpartnern vorab ausgehändigt. Diese konnten sich so entsprechend vorbereiten und es war transparent, was genau der Inhalt des Interviews sein soll. Weiter dienten die Fragen zur Strukturierung der Interviews. Die Fragen wurden mit kleinen Anpassungen über alle Interviews beibehalten.

4.2.1 Interviewfragen

Die Fragen wurden in drei Bereiche aufgeteilt. Zum Einstieg wurden allgemeine Fragen zu IT-Controlling sowie IT-Risikomanagement gestellt. Erst dann interessierten spezifische Fragen zur Integration der Bereiche. Für Sachverständige von Software wurden zusätzliche Frage formuliert.

4.2.1.1 Fragen zum IT-Controlling

„Besteht ein Firmenweites Konzept für das IT Controlling?“

„Wird ein etabliertes Framework wie COBIT, ITIL oder ARIS eingesetzt?“

„Welche Aufgaben hat das IT Controlling und wie ist es ausgestaltet?“

„Wie sehen das strategische sowie das operative Controlling aus?“

„Wie werden die Daten aus dem operativen IT-Controlling (z.B. Projektcontrolling) ins strategische IT Controlling übernommen?“

„Welche spezifischen (IT)-Controlling Tools kommen dabei zum Einsatz?“

„Wo liegen die Hauptprobleme im IT-Controlling?“

4.2.1.2 Fragen zum IT-Risikomanagement

„Besteht ein Firmenweites Konzept für das Risikomanagement?“

„Werden Risken aus den Bereichen IT-Applikationen/Betrieb/Projekten/Strategie erfasst?“

„Wie ist das Risikomanagement für diese Bereiche ausgestaltet?

„Welche spezifischen Risikomanagement Tools kommen dabei zum Einsatz?“

„Wie werden die Risiken aus den Bereichen aggregiert?“

„Wie werden die Daten aus dem operativen Risikomanagement (z.B. Projektrisiken) ins strategische Risikomanagement (z.B. Portfoliorisiken) übernommen?“

„Wo liegen die Hauptprobleme im Risikomanagement?“

4.2.1.3 Fragen zur Integration beider Bereiche

„Wie werden die Daten aus dem IT-Controlling ins Risikomanagement übernommen?“

„Bestehen interne Richtlinien bei der Integration oder wird dabei nach einem anerkannten Standrad gearbeitet?“

„Besteht ein (internes) Datenmodell welches die Integration erleichtert?“

„Verschiedne Personen interpretieren die gleichen Daten unterschiedlich und erzeugen damit Fehlinterpretationen. Wie wird dem Problem begegnet?“

„Verschiednen Personen messen den gleichen Daten unterschiedliche Relevanz bei und erzeugen damit divergente Interpretationen. Wie wird dem Problem begegnet?“
„Werden durchgängig die gleichen Tools verwendet?“
„Welche Anforderungen stellen Sie an ein Integrationskonzept?“

4.2.1.4 Für Sachverständige entsprechender Software

„Auf welchen Konzepten/Datenmodellen basiert der integrative Ansatz der Software“
„Basiert der Integrative Ansatz auf einem bereits anerkannten Ansatz oder handelt es sich um eine Eigenentwicklung?“
„Ist das Modell nach welchem die Integration erfolgte für den Anwender transparent?“

4.3 Adressaten des Interviews

Mögliche Adressaten finden sich am ehesten in folgenden Bereichen:

- IT-Leiter
- Controller
- IT-Controller
- Consultants
- IT-Risikomanager
- Security Verantwortliche
- Software Sachverständige

Insgesamt wurden 8 Personen aus folgenden Firmen interviewt:

Firma	Befragung im Bereich
ABN Amro Bank	IT-Controlling
Ernst & Young	Consulting / Prüfung Risikomanagement
Fuchs Informatik	Projektconsulting
IBM	IT-Projektcontrolling / IT-Risikocontrolling
Telekurs	Risikomanagement
UBS	IT-Controlling

Tabelle 3: Interviewpartner Befragung

4.4 Durchführung der Interviews

Die Befragung wurde offen geführt. Das heisst, die oben in 4.2 zusammengestellten Fragen wurden nicht der Reihe nach durchgearbeitet, sondern der Situation angepasst gestellt. Aus Verständnisgründen war auch der Einblick in das praktische

Vorgehen der täglichen Arbeit der Interviewpartner von zentraler Bedeutung. Die Interviews wurden, wenn erlaubt, aufgezeichnet.[50] Die Dauer der Interviews lag zwischen einer und drei Stunden. Die Informationsbereitschaft der Interviewpartner war ausserordentlich positiv. Die einzelnen Interviews sind dem Anhang zu entnehmen.

4.5 Auswertung der Interviews

Von jedem Interview wurde ein formloser Transkript erstellt.[51] Sie dienten als Input für die Anforderungen an einen Integrationsansatz. Im folgenden sollen einige bemerkenswerte Konzepte sowie der Stand der Integration von IT-Controlling und IT-Risikomanagement dargestellt werden.

4.5.1 Stand der Integration

Generell zeigt sich ein heterogenes Bild. Nicht nur hinsichtlich auf die Integration an sich, sondern auch hinsichtlich der Konsistenz der verwendeten Begriffswelt. Dieser Punkt wird in 4.5.2.2 genauer dargestellt. Eine bewusste Integration der Bereiche ist nicht auszumachen. Vielmehr wird meistens unkoordiniert versucht, Teilbereiche miteinander zu verknüpfen. Zwar werden oben besprochene Konzepte wie CobIT, ITIL, ARIS oder ISO 17799 verwendet, jedoch nur immer in spezifischen Bereichen. Eine weitergehende Integration ist so nicht möglich.

4.5.2 Merkenswerte Konzepte

Im folgenden soll nicht jedes Detail der Interviews vorgestellt werden. Vielmehr interessieren konzeptuelle Erkenntnisse aus der Praxis. Details zu den Interviews sind in den Audioaufzeichnungen sowie den Transkripten enthalten.

4.5.2.1 Bezug zum Qualitätsmanagement

Obwohl es beim Qualitätsmanagement um das Management von wichtigen Risiken geht, wird Qualitätsmanagement meist völlig losgelöst vom Risikomanagement betrieben. Operativ werden Ereignisse mit hoher Eintretenswahrscheinlichkeit mittels dem Qualitätsmanagement gesteuert. Ereignisse mit tiefer Eintretenswahrscheinlichkeit fallen unter das Risikomanagement.[52] Abbildung 13

[50] [INTERVIEWAUFZEICHNUNGEN]
[51] [INTERVIEWTRANSKRIPTE]
[52] siehe [INTERVIEWAUFZEICHNUNGEN], [INTERVIEWTRANSKRIPTE]

gibt diesen Sachverhalt wieder. Die Bezeichnung Risiko ist dabei im Sinne von Gefahren zu verstehen.

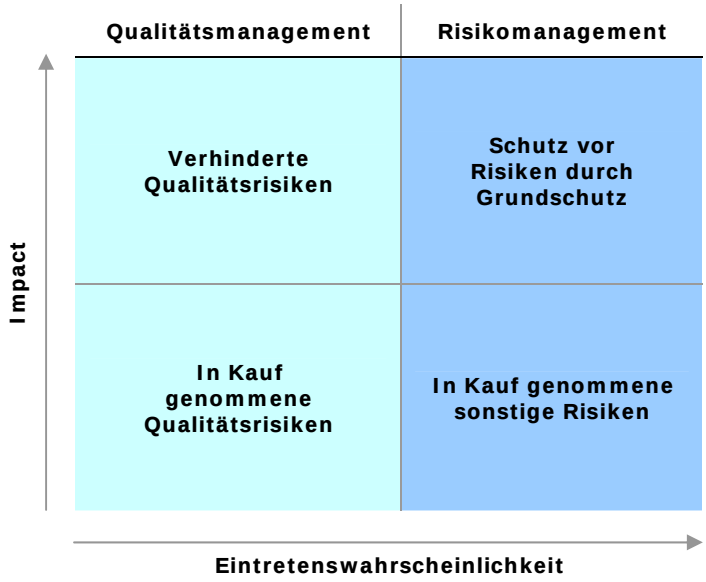

Abbildung 13: Abgrenzung Qualitätsmanagement & Risikomanagement

4.5.2.2 Abgrenzungsprobleme

Dehnt man die in Abbildung 13 gemachten Erkenntnisse auf weitere Gebiete aus, so stellt sich heraus, dass die in Abbildung 14 gezeigten Gebiete sehr stark zusammenhängen. Dies hat starke Implikationen auf das zu erstellende Integrationskonzept und muss dort entsprechenden Niederschlag finden.

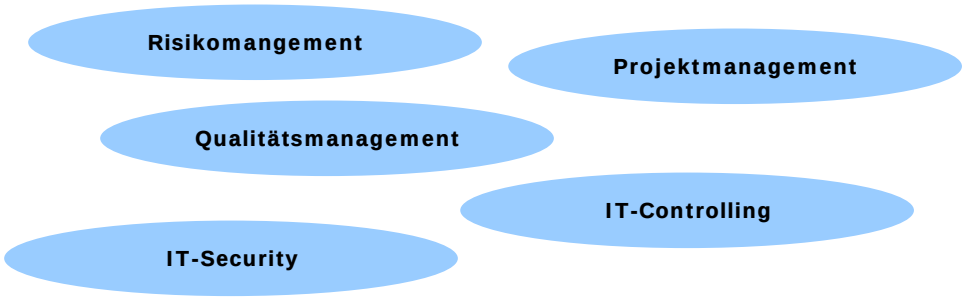

Abbildung 14: Abgrenzungsprobleme & starke Vernetztheit

4.5.2.3 IT-Controlling, Risikomanagement und Audit

Neben der Integration von Risikomanagement und IT-Controlling ist es sinnvoll, auch den Auditbereich miteinzubeziehen. Diese Forderung wurde von mehreren Interviewpartnern erhoben. Es ergäbe sich dann eine Integration von drei Bereichen, welche in weiten Bereichen die gleichen Daten benötigen. Dieser Aspekt wird nochmals in 5.3.9 aufgegriffen.

4.5.2.4 Zielorganisation einer Integration

Ein Integrationskonzept für IT-Controlling und IT-Risikomanagement scheint zunächst nur etwas für Grossfirmen zu sein. Grossfirmen haben viele Systeme und Projekte und bereits oft ein Risikomanagement sowie ein gutes IT-Controlling. Grossfirmen könne also eher vom Effizienzgewinn einer Integration profitieren.
KMU's mit wenigen Systemen und Projekten haben erfahrungsgemäss ein eher moderat ausgebildetes Risikomanagement und ein rudimentäres IT-Controlling. Ein KMU profitiert deshalb eher von erhöhter Effektivität. Das Integrationskonzept ist für KMU's eher ein Rahmen, an welchem Orientierung möglich ist.

5 Ausgestaltung eines Integrationskonzeptes

Im folgenden soll ermittelt werden, inwieweit die in 3.4 und 3.5 vorgestellten Standards als Basis für ein Integrationskonzept im IT-Controlling und IT-Risikomanagement dienen können. Fehlende Aspekte sollen in 5.4 und 5.5 ergänzt werden.

5.1 Integrationsstrategien

Integration bedeutet meistens auch eine Formalisierung von Abläufen. Integrationen kann auf technischer Ebene fixiert werden durch Einführung integrativer Softwarelösungen. Integrationen kann aber auch erreicht werden mittels Durchsetzung organisationsweiter Richtlinien.
Eine interessante Parallele findet sich in Lawrence Lessings Buch ‚Code and Other Laws of Cyberspace'[53], in welchem er die Regulation des Internet aufteilt in Regulation durch Gesetze (Parallele: Regeln in der Unternehmung) und Regulation durch Gestaltung von Code. Unter Code sind bei Lessing Programme, Parametrisierungen oder verwendete Protokolle zu verstehen.

5.1.1 Softwaretechnisch

Wird die Integration verschiedener Systeme über die Einführung von Softwarelösungen vorgenommen, ist der Anwender meist gezwungen die neue Applikation zu benutzen. Die Vorgaben, wie die Integration aussehen soll ist fest in Form von Code[54] einprogrammiert oder parametrisiert[55]. Ein Teil der Durchsetzung

[53] [LESSING00]
[54] Eigenentwicklungen

der Integrationslösung ist damit einfacher. Das bedeutet aber nicht, dass keine Wiederstände für die Integration zu erwarten sind. Die feste Einprogrammierung der Integrationsregeln ist eher unflexibel, auch wenn eine gewisse geplante Flexibilität bei der Programmierung durchaus einkalkuliert werden kann. Änderungen können meistens nur über einen Änderungsantrag vorgenommen werden. Durch die mangelnde Flexibilität kann somit auf Anforderungsänderungen schlecht reagiert werden.

5.1.2 Weisungstechnisch

Werden die Funktionalitäten einer Integration nicht fest einprogrammiert oder parametrisiert bleibt mehr Flexibilität. Auf veränderte Anforderungen kann so schneller reagiert werden. Eine solche Einführung kann auf Ebene von Weisungen stattfinden. Die Benutzer sind dann angehalten diese umzusetzen, unterliegen aber keinem Zwang. Die Durchsetzung ist hier entsprechend schwierig.

5.1.3 Zwischenweg

Ein Kompromiss besteht in der Einführung von Standards nach welchen gearbeitet werden soll. Diese Standards müssen durch entsprechende Technologien unterstützt werden. Wenn ein Anwender die Technologie benutzt, zwingt das den anderen Anwender in gewissem Rahmen auch zu deren Einsatz. Ein Beispiel ist die grosse Verbreitung von Excel. Werden Daten im Excelformat geliefert, muss der Empfänger das gleiche Format verwenden.

Die Durchsetzung des Standards müsste mit Weisungen unterstützt werden. Es ist denkbar, dass ein Organisationsweites Datenmodell zwar festgeschrieben, dies aber nicht in Form von festen Applikationen durchgesetzt wird. Vielmehr ist das Datenmodell dann Hilfsmittel für den alltäglichen reibungslosen Datenaustausch. Das Datenmodell könnte in XML gehalten sein.

5.2 Anforderungen an ein Integrationskonzept

5.2.1 Schematische Übersicht

Das Ziel einer Integration von IT-Controlling und Risikomanagement ist die Erfüllung der Anforderungen. Aus den Problembereichen ergeben sich die Anforderungen an ein Integrationskonzept für IT-Controlling und IT-

[55] z.B. SAP Systeme

Risikomanagement. Die Anforderungen sind in Abbildung 15 in einer schematischen Übersicht zusammengestellt. An oberster Stelle steht dabei das Kriterium der Wirtschaftlichkeit. Alle anderen Anforderungen sind der Wirtschaftlichkeit untergeordnet, haben darauf aber einen mehr oder weniger starken Einfluss. Die primäre Anforderung der Wirtschaftlichkeit kann auch als Formalanforderung, die sekundären als Sachanforderung interpretiert werden. Direkt beeinflusst werden kann die Wirtschaftlichkeit nur über die Steuerung der Sachanforderungen.

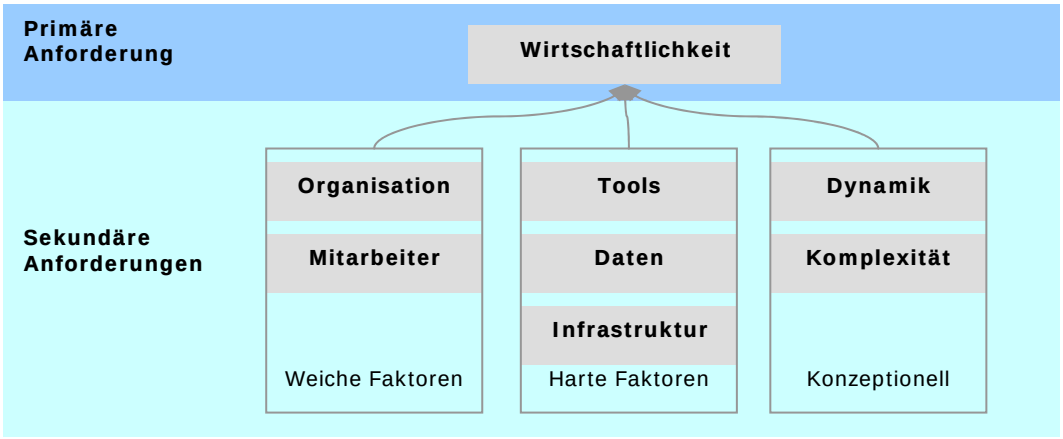

Abbildung 15: Anforderungen an ein Integrationskonzept

5.2.2 Anforderungen

Aus der Analyse der Problemfelder aus 3.6 ergeben sich die in Tabelle 4 zusammengestellten Anforderungen an eine Integration von IT-Controlling und IT-Risikomanagement.

Problmebereich	Anforderung
Organisation	Die Organisationsform (zentral, dezentral), die Organisationsgrösse sowie die Unternehmenskultur müssen berücksichtig werden.
Mitarbeiter	Mögliche personelle Wiederstände aufgrund von Machstrukturen und divergenten Interessen müssen berücksichtigt werden.
Infrastruktur	Der Trade-off zwischen alter, günstiger, aber funktional eingeschränkter Infrastruktur und neuer, teurer, dafür flexiblen und funktional vielseitiger Infrastruktur muss optimal gelöst werden.
Daten	Sichergestellt werden muss die Datenverfügbarkeit (technisch, personell und zeitlich), die Richtigkeit der Daten, die Wirtschaftlichkeit der Datenbeschaffung, die Vertraulichkeit der Daten sowie die Möglichkeit des Einbezuges externer Daten. Unklarheiten in der Semantik und der individuellen Einschätzung der Relevanz von Daten müssen ausgeräumt werden. Die Datenqualität muss den Anforderungen an IT-Controlling und Risikomanagement genügen.
Tools	Der Einsatz von Tools soll möglichst homogen sein. Die Tools müssen die geforderten Funktionen zuverlässig erfüllen.
Dynamik	Auf wechselnde Anforderungen muss schnell und flexibel reagiert werden können, ohne dabei komplizierte Änderungsprozeduren in

Problmebereich	Anforderung
	Gang zu setzten, welche die Veränderungen behindern würden. Im Trade-of von Flexibilität und Stabilität muss das Optimum gefunden werden. Im Falle von regulatorischen Änderungen muss das Integrationskonzept genug flexibel sein, um schnell und angemessen reagieren zu können. Auf neue Produktportfolios und veränderte Marktbedingungen muss schnell und angemessen reagiert werden können.
Komplexität	Auch für komplexe Sachverhalte sollen die Vorteile der Integration wirksam sein. Es darf nicht sein, dass komplizierte Dinge plötzlich ad-hoc erledigt werden.
Wirtschaftlichkeit	Vor der Durchsetzung eines Integrationskonzeptes muss die Frage der Wirtschaftlichkeit beantwortet werden. Auch wenn die Quantifizierung schwer fällt, ist dieser Schritt unumgänglich. Auch Teilschritte müssen der Frage der Wirtschaftlichkeit unterzogen werden.

Tabelle 4: Anforderungen an ein Integrationskonzept

5.3 Brauchbarkeit bestehender Konzepte

Nachdem einerseits verschiedene Konzepte in 3 vorgestellt und andererseits die Anforderungen an ein Integrationskonzept für IT-Controlling und Risikomanagement in 5.2 definiert wurden, kann nun beurteilt werden, welches Konzept für eine Integration von IT-Controlling und IT-Risikomanagement verwendet werden kann.

5.3.1 Evaluation

In Tabelle 5 wird in einer kurzen Übersicht dargestellt, welche Anforderungen von welchem Konzept erfüllt werden.

Problem-bereich	Anforderungen werden erfüllt von				
	CobIT	ITIL	ISO 17799	ARIS	XBRL
Organisation	⊙	○	⊙	◉	○
Mitarbeiter	⊙	○	⊙	○	○
Infrastruktur	⊙	○	◉	⊙	⊙
Daten	◉	⊙	○	⊙	◉
Tools	○	○	○	◉	◉
Dynamik	⊙	⊙	⊙	⊙	◉
Komplexität	⊙	⊙	○	⊙	◉
Wirtschaftlichkeit	⊙	◉	⊙	⊙	◉

Symbole:
◉=Anforderungen werden weitgehend erfüllt
⊙=Anforderungen werden teilweise erfüllt
○=Anforderungen werden nicht erfüllt

Tabelle 5: Evaluation bestehender Konzepte

Die untersuchten Frameworks wie Cobit, ITIL, ISO 17799 oder ARIS bieten keine geeignete Basis für eine Integration. Probleme, wie sie bei einer Integration zu erwarten sind (siehe 3.6) werden nur sehr begrenzt gelöst, beziehungsweise gar nicht behandelt. Besser ist der XML basierte, technische Standard XBRL. XBRL deckt aber nur technische Aspekte und Fragen der Standardisierung ab. Weiche Faktoren werden erwartungsgemäss nicht behandelt.

5.3.2 Evaluation von XML/XBRL

Neben den organisatorischen und menschlichen Problemen gehören technische, schnittstellenspezifische Probleme zu den Hauptproblemen einer Integration von IT-Controlling und Risikomanagement. Es ist daher nicht erstaunlich, dass XBRL als technischen Standard einen guten Beitrag zur Lösung der technischen Schnittstellenproblemen leisten kann. Folgende Anforderungen werden von XBRL erfüllt:

5.3.3 Erfüllung der Anforderungen betreffend Infrastruktur

Aufgrund der Standardisierung von XBRL[56] und der Tatsache das XBRL auf XML basiert, werden die Anforderungen an die Infrastruktur reduziert. Es muss nicht für jede Applikation eine spezielle Middleware geschrieben werden. Ältere Software kann um eine XML Schnittstelle erweitert werden, welche auch für andere Zwecke eingesetzt werden kann. Der Aufwand ist zwar erheblich, verteilt sich aber.

5.3.4 Erfüllung der Anforderungen betreffend Daten

Hier liegt das Hauptpotential von XBRL. Die *Datenbeschaffung* wird durch die Standardisierung erleichtert und damit wirtschaftlicher, vorausgesetzt die richtigen Dinge wurden im richtigen Ausmass standardisiert. Weiter wird der *Einbezug externer Daten* erleichtert. Liegen diese auch bereits als XBRL File oder zumindest als XML File vor, so lassen sich diese effizient kombinieren, ohne sich um Datenformate kümmern zu müssen. *Semantische Unklarheiten* werden mit XBRL ebenso minimiert. XML und damit auch XBRL ermöglichen durch die Angabe von Namespaces eine Festlegung der Semantik von Daten. Durch die Klarheit der Bedeutung von Daten wird auch das Risiko minimiert, Daten eine unterschiedliche Relevanz beizumessen. Allerdings bleibt hier ein beträchtlicher Interpretationsspielraum, kein Standard kann den vollständigen Kontext von Daten

[56] Aktuell in Version 2.0a verfügbar gemäss http://www.xbrl.org/resourcecenter

abbilden. Eine weitere Folge der Reduktion von semantischen Unklarheiten ist eine *Erhöhung der Datenqualität*. Unabsichtliche Fehleingaben oder falsche Werte entstehen weniger, da die Bedeutung der Daten im Zweifelsfall über Referenzen verfügbar ist.

5.3.5 Erfüllung der Anforderungen betreffend Tools

Der XBRL Standard schreibt keine Tools vor, weil dies auch nicht nötig ist. XML ist tool-, und herstellerunabhängig. Damit kommt jedes Tool, welches den XML Standard beherrscht auch mit XBRL Files zurecht. Ein homogener Einsatz von Tools ist jedoch trotzdem effizienter. Wo dies aber nicht möglich ist, trägt XBRL zur Entschärfung des Problems bei. Tools die zwar XML unterstützen, aber möglicherweise in einer alten oder herstellerspezifischen Version oder in einer fehlerhaften Implementation vorliegen, sind eine Gefahr für den effizienten XBRL Einsatz.

5.3.6 Erfüllung der Anforderungen betreffend Dynamik

Durch die Standardisierung in XML kann schnell auf wechselnde Anforderungen reagiert werden, ohne komplizierte Änderungsprozeduren in Gang zu setzten, wie z.B. die Umprogrammierung von Middleware. Allerdings müssen entsprechend Schemas oder Taxonomien angepasst werden.

5.3.7 Erfüllung der Anforderungen betreffend Komplexität

Vorausgesetzt, Schemas und Taxonomien sind flexibel definiert, so können effizient sowohl einfache als auch komplexe Anforderungen befriedigt werden.

5.3.8 Erfüllung der Anforderungen betreffend Wirtschaftlichkeit

Die genannten Anforderungen haben zuletzt eine Verbesserung der Wirtschaftlichkeit zum Ziel. Sind die untergeordneten Punkte erfüllt, so ist auch die Anforderung nach erhöhter Wirtschaftlichkeit insgesamt erfüllt. Der Gedanke der Wiederverwendung steht dabei im Zentrum. Wiederverwendet werden kann ein flexibles Datenmodell, nicht aber eine XBRL-Taxonomie die nicht erweiterbar ist.

5.3.9 Was leistet XBRL für ein Integrationskonzept?

XBRL kann als Basis für die Entwicklung eines Integrationskonzepts dienen. Was XBRL dabei konkret leistet, ist in den Abschnitten 5.3.3 bis 5.3.8 aufgeführt. XBRL als Sprache für das externe Reporting ist für das interne IT-Controlling und das Risikomanagement im aktuellen Entwicklungsstadium nur begrenzt einsetzbar. Der Standard müsste entsprechend um spezifische Taxonomien erweitert werden. Ist die Erweiterung einmal geleistet, bildet XBRL ein standardisiertes Datenmodell ab, mit dem zusätzlichen Vorteil, dass die Daten dann sowohl einheitlich für das interne Reporting als auch für das externe Reporting benutzt werden können. Dieser Aspekt ist wichtig, wenn man die Integration weiter führen will in Richtung Audit und Revision. Darin würde möglicherweise noch mehr Potential liegen. Diese weiterführende Erweiterung des Integrationsansatzes mit XBRL soll hier aber nicht behandelt werden.
XBRL bietet aber für eine Reihe von Problemen keine Lösung. Diese Einschränkungen sollen im Folgenden Abschnitt behandelt werden.

5.3.10 Was kann XBRL nicht leisten?

Da XBRL ein technischer Standard ist, können organisatorische oder personelle Probleme nicht angegangen werden. Auch andere Problembereiche wie z.B. die Wirtschaftlichkeit oder der Infrastruktur werden in XBRL nicht explizit behandelt. Die Technologie und die zugrundeliegenden Taxonomien haben aber sicher grossen Einfluss auf die genannten Problembereiche.

5.3.11 Notwendige Erweiterungen

Die meisten Erweiterungen erfolgen sinnvollerweise ausserhalb des XBRL Standards, sind es doch meist nicht technische Anforderungen. Dazu zählen Bereiche wie Organisation, Personal oder Infrastruktur. Nur die eher technischen Erweiterungen sollten innerhalb des XBRL Standards erfolgen. Dazu gehören notwendige Erweiterungen im Bereich der Taxonomien. Im folgenden werden diese Erweiterungen diskutiert. Das erweiterte Framework wird im weiteren mit ‚Extended_XBRL' benannt. Die vorliegende Arbeit konzentriert sich auf die Erweiterungen innerhalb von XBRL.

5.3.11.1 Erweiterungen ausserhalb XBRL

Damit auf Basis von XBRL ein Konzept für die Integration von IT-Controlling und IT-Risikomanagement erstellt werden kann, müssen wie bereits in 5.3.9 angedeutet folgende Bereiche mit einbezogen werden.

Organisatorische Aspekte

Einbezug der Anforderungen organisatorischer Hinsicht gemäss *5.2*

Mitarbeiter

Einbezug der Anforderungen personeller Hinsicht gemäss *5.2*

Infrastruktur

Kriterien für den optimalen Einsatz von alter und neuer Infrastruktur

Daten

Die Anforderungen an die Daten sind im CobIT Standard sehr gut strukturiert. Diese Strukturierung kann in Formulierungen eines Integrationskonzeptes miteinbezogen werden.

Tools

Eine zuverlässige Verarbeitung von Daten kann nur mit einwandfrei funktionierenden und spezifikationskonformen Tools sichergestellt werden. Dies kann durch zertifizierte Tools erfolgen, welche von XBRL.org [57] oder vom W3 Konsortium [58] erstellt werden könnte. Steht eine solche nicht zur Verfügung, wie aktuell der Fall, besteht die Möglichkeit von Unternehmensinternen Prüfungen.

Wirtschaftlichkeit

Kriterien zur wirtschaftlichen Implementierung von Extended_XBRL (und XBRL im allgemeinen) wären wünschenswert. Ein Kriterienkatalog könnte von XBRL.org erstellt werden.

XML basierte Standards bieten Vorteile bei klarer Semantik der Daten. Strukturen lassen sich sehr dynamisch anpassen und kommen so auch den Bedürfnissen von komplexen Anforderungen entgegen. Die Kriterien um die Themenbereiche Daten, Dynamik sowie Komplexität werden bereits gut in XBRL und XML abgedeckt, trotzdem sind Erweiterungen notwendig. Diese Erweiterungen folgen nun.

[57] [XBRL_INTERNATIONAL]
[58] [W3C]

5.3.11.2 Erweiterungen innerhalb XBRL

Sollen die Anforderung betreffend Daten, Dynamik und Komplexität erfüllt werden, so muss XBRL selbst erweitert werden, dabei sind primär Erweiterungen in der Taxonomie[59] gemeint.

Bisher wird XBRL primär für das externe Reporting eingesetzt, d.h. der rechte, helblaue XBRL-Balken in Abbildung 16. Siehe hierzu auch Abbildung 11. Soll auch im internen Reporting XBRL zum Einsatz kommen, erweitert sich die Architektur um den linken, gelben Extended_XBRL-Balken. Dabei würden die Daten aus den Vorsystemen, z.B. Datenbanken oder Transaktionssystemen als XML File geliefert. Anderseits fände der Austausch von Daten im internen Reporting über Extended_XBRL statt.

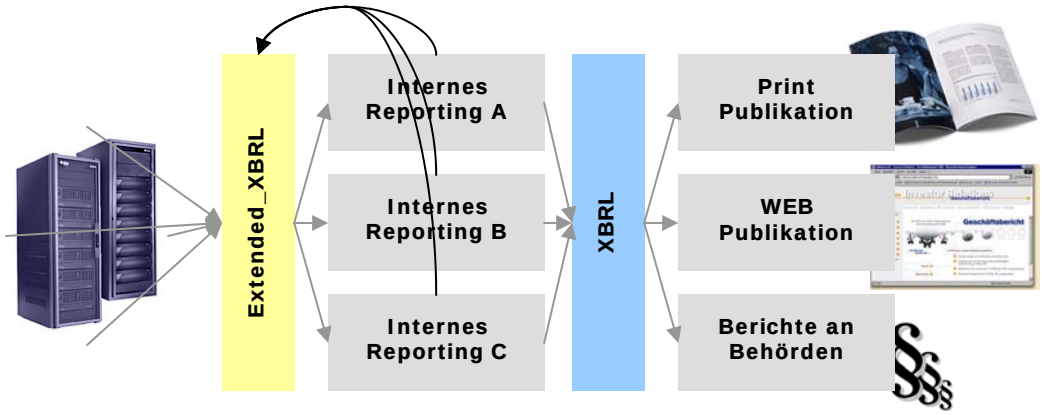

Abbildung 16: erweiterte XBRL Architektur unter Einbezug des internen Reportings

Nutzen

Die Informationsempfänger müssen sich nur noch auf ein Datenformat einstellen. Die Daten liegen in einem einheitlichen, logischen Datenschema vor. Die mühsame, manuelle Aufbereitung entfällt so zum grössten Teil. Die Integration von bestehenden Daten und Auswertungssystemen lässt sich vereinfachen. Der Informationsfluss wird vereinfacht und effizienter. Fehlerquellen werden aufgrund der klaren Semantik minimiert.

Taxonomieerweiterungen

Folgende Bereiche müssen in eine erweiterte XBRL einfliessen:

[59] Der Begriff Taxonomie wird von XBRL.org verwendet, gemeint ist die mit semantischen Informationen versehene Datenstruktur

- Taxonomieerweiterung für IT-Controlling
- Taxonomieerweiterung für IT-Risikomanagement

Die zu erstellenden Taxonomien müssen unbedingt unter sich, als auch mit den bestehenden XBRL Taxonomien kompatibel sein. Die Erweiterung könnte auch unabhängig vom Standard firmenspezifisch erfolgen, mit dem Nachteil, dass jede Unternehmung den gleichen Aufwand betreiben muss. Der Anspruch auf XBRL-Kompatibiltät kann in der vorliegenden Arbeit noch nicht eingelöst werden.

Im folgenden soll ein Vorschlag für eine geeignete Taxonomie verfasst werden. Ziel soll nicht sein, eine vollständige erweiterte Taxonomie zu erstellen. Hierzu wäre eine langwierige Expertendiskussion mit anschliessendem Konsens notwendig. Hier soll nur das prinzipielle Funktionieren des Ansatzes gezeigt werden. Dabei können nur vereinzelte Elemente berücksichtigt werden. Es ist nicht Aufgabe dieser Diplomarbeit, eine vollständige Kompatibilität mit dem XBRL Standard herzustellen. Vielmehr soll anhand eines kleinen Ausschnittes aus dem internen Controlling gezeigt werden, wie eine XML basierte Notation der Daten abläuft und wie dabei die Integration von IT-Controlling und IT-Risikomanagement realisiert werden kann.

5.4 Taxonomie IT-Controlling

5.4.1 Anforderungen

Im Gegensatz zu externen Reportingdaten in XBRL muss im Controlling einer Ist-Position immer eine Soll-Position gegenübergestellt werden. Da die Sollpositionen und die Istpositionen nicht immer von den gleichen Instanzen bearbeitet werden, müssen diese getrennt erfasst werden können. Das hat Implikationen auf die Definition erforderlicher Elemente.

Jedes Kontrollergebnis ist das Resultat eines Soll/Ist Vergleiches. Abweichungen können als Risiken interpretiert werden. Diese Risiken sind Chancen oder Gefahren, welche sich entsprechend auf das Ergebnis der Organisationseinheit auswirken. Umgekehrt bestehen aber auch Risiken, welche nicht direkt auf eine festgestellte Abweichung aus dem IT-Controlling zurückzuführen sind. Auch solche Risiken

(Gefahren *und* Chancen) müssen in die zu erstellende Taxonomie passen. Dieses Konzept ist in Abbildung 17 dargestellt.

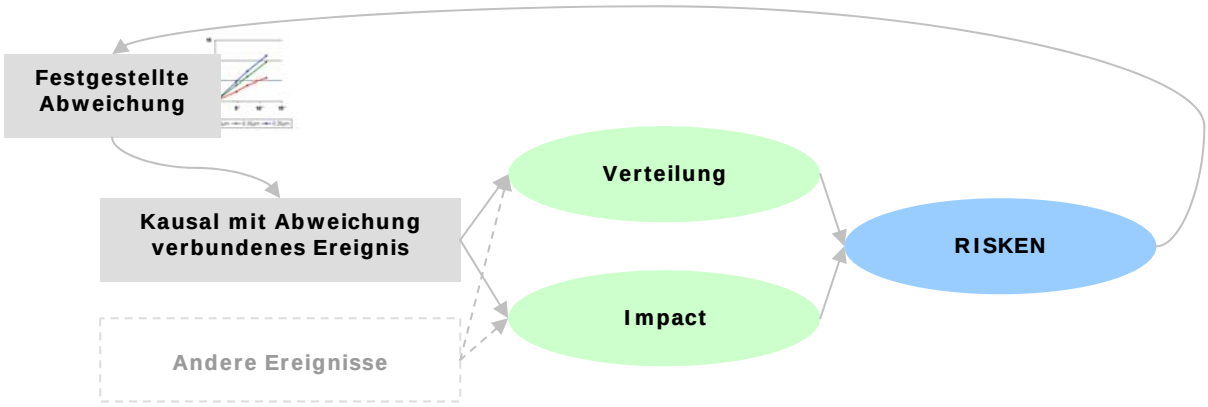

Abbildung 17: Zusammenhang Controlling & Risiko

5.4.2 Modellierung

Konkret wird ein Beispiel aus dem Projektcontrolling eines Entwicklungsprojektes aufgegriffen. Dabei wird ein vereinfachtes Projektcontrolling abgebildet. So wird unter dem Punkt der Budgetkontrolle das gesamte Projektbudget subsummiert. In der Praxis muss das entsprechend verfeinert werden.

- Objektdaten (Name, Periode, Verantwortlichkeit)
- Budgetkontrolle (Soll, Ist, Abweichung)
- Projektfortschrittkontrolle (Soll, Ist, Abweichung[60])
- Personalressourcenkontrolle (Soll, Ist, Abweichung)
- Terminkontrolle (Soll, Ist, Abweichung)
- Qualitätskontrolle (Soll, Ist, Abweichung)

Die unten aufgeführte Abbildung 18 visualisiert das zugrunde liegende Datenmodell zum IT-Projektcontrolling.

[60] Hat Implikationen auf die Aktivierungsfähigkeit nach IAS, siehe hierzu [KRCMAR00]

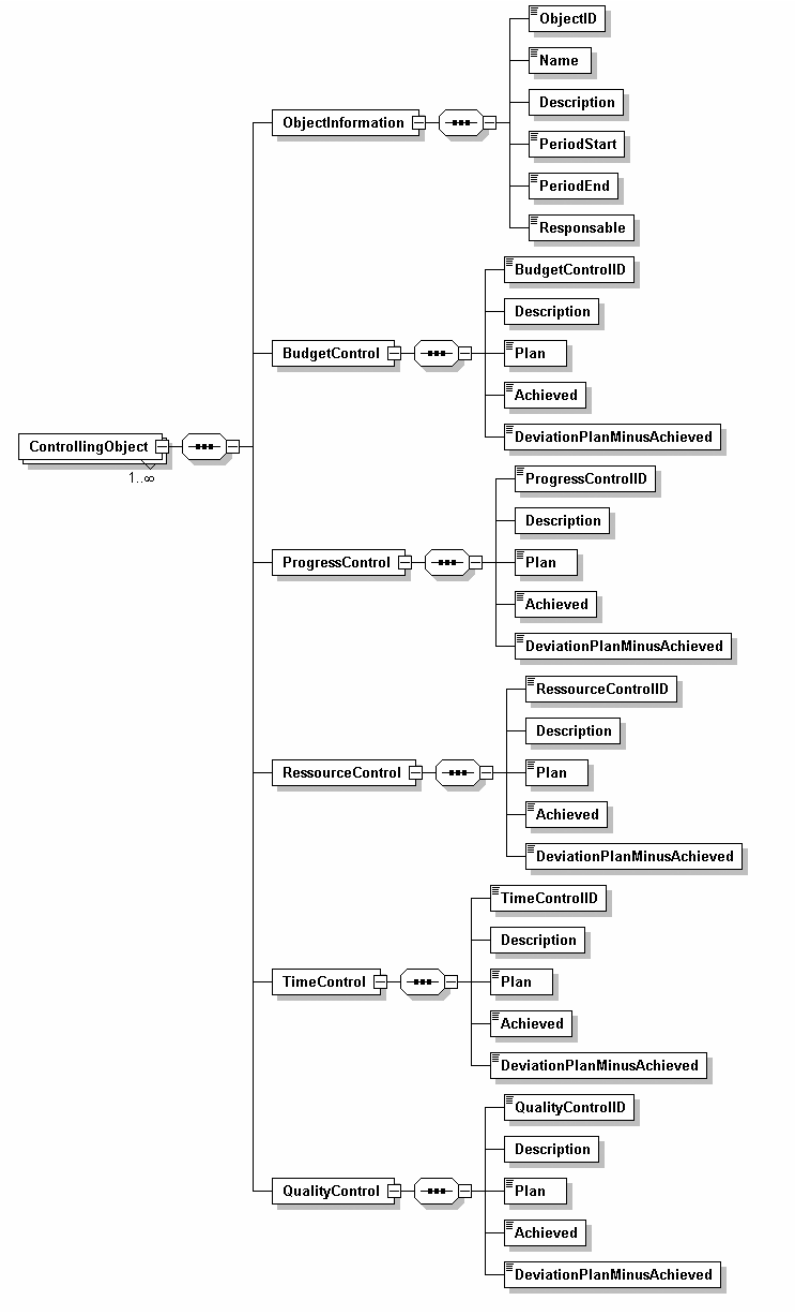

Abbildung 18: Datenmodell IT-Controlling, Ausschnitt aus dem Projektcontrolling

5.5 Taxonomie IT-Risikomanagement

5.5.1 Abhängigkeit vom IT-Controlling

Risiken können gemäss Abbildung 17 aus Abweichungen von Controllingobjekten[61] resultieren. Risiken können aber auch auf externe Faktoren zurückführbar sein. Die hier zu erstellende Taxonomie für Risiken soll auf beide Arten Rücksicht nehmen. Im

[61] Ein Controllingobjekt ist der Sachverhalt, welcher durch die Controllingmassnahme überwacht wird.

ersten Fall ist die Risikobetrachtung Teil des Controllingobjektes. Im zweiten Fall besteht das Risiko losgelöst von einem bereits bestehenden Controllingobjekt.

5.5.2 Modellierung

- Objektdaten (Risikobezeichnung, Periode, Verantwortlich)
- Bezug zu Controllingobjekt (fakultativ)
- Verbund mit anderen Risiken (fakultativ)
- Impact (Maximaler Impact, Definition ob Upside- und Downsiderisk als positive/negative Werte)
- Wahrscheinlichkeit des Ereigniseintritts (Verteilung, Erwartungswert)

Die unten aufgeführte Abbildung 19 visualisiert das zugrunde liegende Datenmodell des Risikomanagements

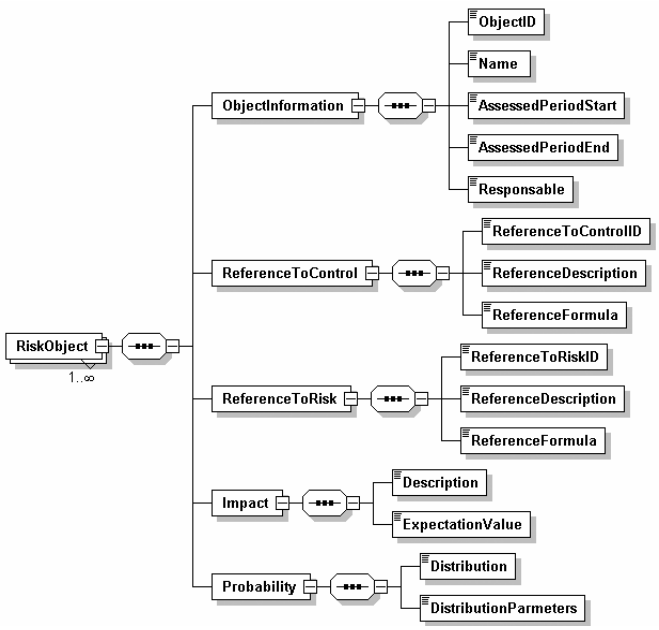

Abbildung 19: Datenmodell IT-Risikomanagement

Neben dem modellierten Erwartungswert interessieren noch andere Werte. Diese sind nicht modelliert, um die Flexibilität möglichst gross zu halten. Meist interessiert auch nur der Erwartungswert. Nur bei Aggregationen und Risikointerdependenzen sind weitere Informationen von Interesse.

5.6 Modellierung der Integration

Wie in Abbildung Abbildung 17 skizziert, sollen IT-Controlling (hier ein Teilbereich aus dem Projektcontrolling) mit IT-Risikomanagement in integrierter Form modelliert werden. Abbildung 20 stellt das integrierte Datenmodell in vereinfachter Form dar. Die in Abbildung 18 und Abbildung 19 vorgestellten Datenmodelle enthalten die jeweiligen Detailsichten von ‚*ControllingObject*' sowie ‚*RiskObject*'.

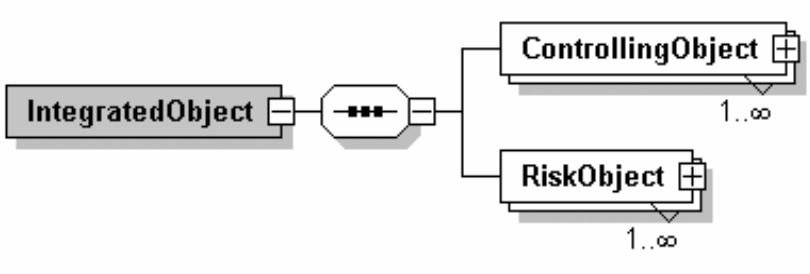

Abbildung 20: Datenmodell Integriertes IT-Controlling und IT-Risikomanagement

Die Funktionsweise der Verlinkung der Controllinginformationen mit den Risiken wird in Abbildung 21 visualisiert. Damit die Verlinkung von einzelnen RiskObjecs gezeigt werden kann, wurde das RiskObject zweimal aufgeführt. Im Datenmodell erscheint es natürlich nur einmal. Im Modell sind *0 bis n* ‚*ControllingObject*' sowie *0 bis n* ‚*RiskObject*' erlaubt.

Der Link von einer Abweichung aus dem Controlling zu einem Risiko wird über eine ID realisiert. Diese ID ist im ganzen Datenbestand eindeutig. Referenzen sind dabei nur unidirektional vom Controllingobjekt zum Risikoobjekt möglich. Weiter können Risiken untereinander verbunden sein (Verbundrisiken). Dazu sind Referenzierungen zu anderen Risikoobjekten möglich. Diese sind bidirektional möglich.

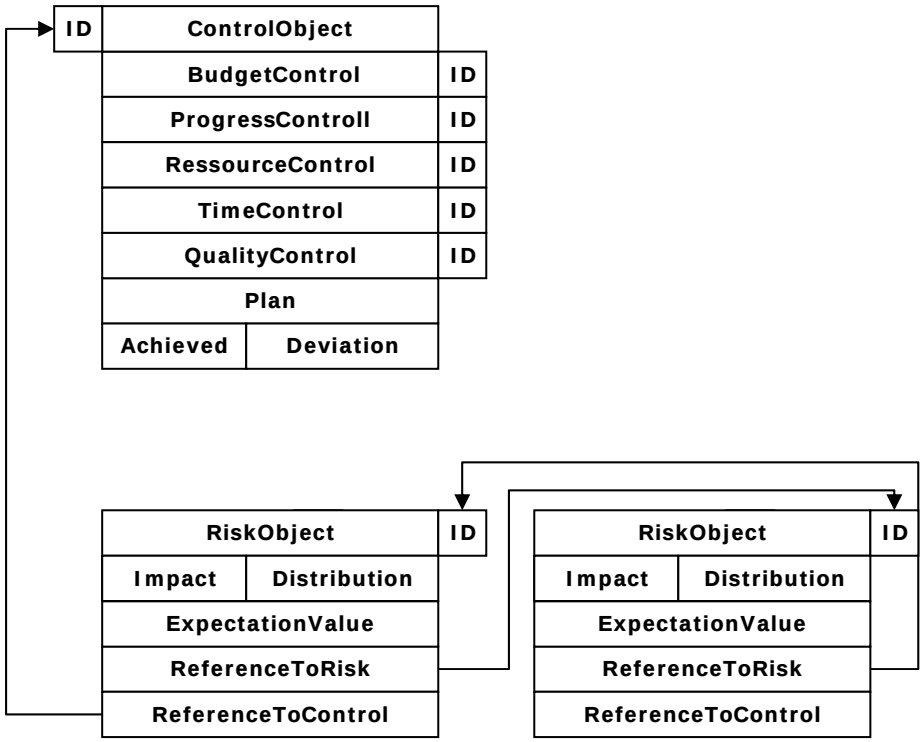

Abbildung 21: Visualisierung der Verlinkung von Controllingdaten und Risiken

5.7 Codierung

Die Codierung erfolgte mittels XMLSPY [62] . Codiert wurde das Schema (Extended_XBRL.xsd) sowie ein Instanzdokument (Extended_XBRL_Instance.xml) welche als Basis für die nachfolgende Verifizierung anhand einer Fallstudie dienen. Beide Dokumente sind im Anhang unter 12.1 angeführt.

5.8 Alternative Modellierung mit RDF und RDFS

Anstelle einer Modellierung mittels XML/XML Schema besteht die Möglichkeit der Modellierung mit RDFs [63] und RDF Schemas. RDFs bieten die Möglichkeit, die Semantik von Daten noch besser zu beschreiben und fördert bei breiter Anwendung die Interoperabilität von XML-Daten. Da gerade das Reporting, sei es externes oder internes Reporting, auf einheitliche Taxonomien angewiesen ist, wären RDFs hier bestens geeignet.

RDF's werden jedoch in XBRL nicht angewandt. Auch im hier vorgeschlagenen Integrationsmodell kommen RDF's nicht zum Einsatz. Der Einbezug von RDFs könnte aber zukünftig sinnvoll eingebaut werden.

[62] [XMLSPY]
[63] Akronym für ‚Ressource Description Framework', Details siehe [W3C]

6 Anwendung in einer Fallstudie

6.1 Ziel

Im folgenden soll anhand von realen Daten gezeigt werden, dass das unter 5.4 und 5.5 erstellte Integrationsmodell, Extended_XBRL, auf reale Daten angewandt werden kann. Weiter soll gezeigt werden, dass die Verknüpfung der Controllingdaten mit Risiken funktioniert. Ein Blick soll auch auf die Brauchbarkeit der zu Verfügung stehenden Tools, sowie auf deren Automatisierungspotential geworfen werden.

Ob das Integrationsmodell alle Anforderungen an ein Integrationskonzept gemäss Tabelle 4 erfüllt, wird hier nicht im Detail erläutert. Diese Arbeit wurde bereits in der Evaluation von XBRL in 5.3.3 bis 5.3.8 geleistet. Die Erkenntnisse lassen sich auf das hier vorgeschlagene Integrationsmodell übertragen.

6.2 Vorgehen

Nach der Zusammenstellung der Daten werden diese entsprechend dem Datenmodell aus 5.6 und dem XML Schema aus 5.7 dargestellt. Nachfolgend werden spezifische Risiken resultierend aus den Controllingabweichungen abgeleitet und ebenfalls Schemakonform dargestellt.

6.3 Daten[64]

Die Daten stammen aus dem Projektcontrolling aus einem SAP-Projekt[65]. Folgende Daten stehen zur Verfügung:

- Objektdaten (Name="SAP-Einfuehrung", Periode="01.07.02 bis 31.07.03", Verantwortlich="Daniel M Schmid")
- Budgetkontrolle (Soll="104'000", Ist="120'000", Abweichung="16'000")
- Projektfortschrittkontrolle[66] (Soll="10", Ist="8", Abweichung="2")
- Personalressourcenkontrolle[67] (Soll="100%", Ist="110%", Abweichung ="10%")
- Terminkontrolle[68] (Soll="2", Ist="1", Abweichung)

[64] [GAULKE02]
[65] SAP Einführungsprojekt in der Versicherungsbranche, Einführung des Moduls ‚Collection and Disbursement' aus dem Bereich Financial Services (FS-CD).
[66] Da sich das Projekt in der Einführungsphase befand, war ein wichtiger Teilaspekt des Projektfortschritts die Anzahl abgenommener Funktionen. Die angegebenen Zahlen sind deshalb abgenommene Funktionen.
[67] Die Kontrolle der Personalressourcen bezog sich auf jeden einzelnen Mitarbeiter. Hier wird die aggregierte Zahl über alle Mitarbeiter eingesetzt.

- Qualitätskontrolle[69] (Soll="0", Ist="5", Abweichung)

6.4 Durchführung

Die Daten wurden manuell unter Zuhilfenahmen des XML Editors XMLSPY in einem Instanzdokument eingegeben. Die automatische Validitätsprüfung sowohl auf korrekte XML Syntax als auch Schemakonformität erleichterte die Arbeit. Bei der Modellierung der Verteilungen der Risiken musste wie üblich im Risikomanagement auf Annahmen über das Eintreten der Ereignisse zurückgegriffen werden. Kausale Zusammenhänge zwischen Controllingergebnissen und Risiken sowie zwischen Risiken untereinander konnten standardisiert festgehalten werden. Beim Schadensausmass konnte der Erwartungswert standardisiert erfasst werden. Die Verteilung wurde bei Bedarf entsprechend modelliert. Die Daten lagen zum Schluss in einem wohl geformten und schemakonformen Format vor und können nun weiter in XML Editoren bearbeitet werden.

6.5 Ergebnisse der Fallstudie

Im folgenden wird beurteilt, inwieweit die in 6.1 festgelegten Ziele erreicht wurden. Dazu wird die in Abschnitt 6.4 geschilderte Durchführung kritisch hinterfragt.

6.5.1 Risikobeurteilung

Die Arbeit der Risikobeurteilung kann auch eine Abbildung in Extended_XBRL nicht leisten. Immerhin wurde ein standardisierter Rahmen für die Abbildung der Risiken zur Verfügung gestellt. Risiken werden in einheitlicher Form dargestellt, eben innerhalb der Semantik von Extended_XBRL. Dies erleichtert eine konsistente Beurteilung von Risiken.

6.5.2 Automatisierung

Die Daten konnten nicht automatisch ins gewünschte Schema eingelesen werden. Hierzu wäre zusätzliche Software wie z.B. GoXML-Transform erforderlich, welche das Mapping erleichtern[70]. Auch für die Weiterverarbeitung in Analysetools für das Risikomanagement muss ein entsprechendes Mapping vorgenommen werden. Mit

---

[68] Die Terminerreichung wurde duch das Erreichen von Meilensteinen kontrolliert. Die Terminkontrolle liegt nahe bei den Informationen der Projektfortschrittkontrolle. Die angegebenen Zahlen sind erreichte Meilensteine.
[69] Ein Mass der Qualitätskontrolle war die Anzahl neuer Störrapporte. Ein Projekt in der Einführungsphase sollte keine neuen Störrapporte generieren. Der Ist-Wert lag trotzdem über Null.
[70] [XMLGLOBAL]

Hilfe von Mappingsoftware können auf einfache Weise Daten von einer Datenstruktur in eine andere übernommen werden. Allerdings müssen diese Strukturen kompatibel sein. Ein weiteres Problem ist der mögliche Verlust von semantischen Informationen. Der Ablauf einer Automatisierung sollte daher genau geregelt werden, ansonsten der Sinn von XML mit seinen Metainformationen verloren geht.
Mit Hilfe von zusätzlichen Tools liesse sich ein Grossteil des Dateninputs sowie -outputs automatisieren.

6.5.3 Berechnungsfunktionalität

Ist Berechnungsfunktionalität gefordert, wie z.B. die Aggregation von Risiken oder Controllingzahlen, so müssen die in XML einheitlich gespeicherten Daten in ein geeignetes Tool importiert werden. Dort können die gewünschten Berechnungen durchgeführt werden. Allenfalls lassen sich die Resultate wie Risikoaggregationen wieder im Extended_EBRL Schema speichern.

6.5.4 Risikointerdependenzen

Referenzen zwischen Controllingobjekten und Risiken liessen sich wie gewünscht modellieren. Nicht modelliert werden konnte eine automatisierte Form von Referenzen, welche Risiken automatisch aus Controllinginformationen berechnet. Die Möglichkeit, Interdependenzen in einer Formel abzubilden, sind Basis für eine nachfolgende automatisierte Berechnung.

6.5.5 Verteilungsmodellierung

Bei der Modellierung der Verteilung des Ereigniseintrittes fehlte auf den ersten Blick die simple Eingabe von maximalem Impact und Eintretenswahrscheinlichkeit, wie in Formel 1 festgehalten. Diese einfache Sichtweise geht von einem maximal möglichen Impact aus. Durch geschickte Wahl der Verteilungsfunktion kann auch diese Situation abgebildet werden, z.B. mit einer Rechtecksverteilung. Verteilungen wie die Normalverteilung kennen im Vergleich dazu keine Ober- oder Untergrenzen des möglichen Impacts. Das vorliegenden Modell deckt also alle Fälle ab, einfache aber auch komplexere Verteilungen.

6.6 Zielerreichung

Es konnte gezeigt werden, dass das integrierte Datenmodell Extended_XBRL auf reale Daten angewandt werden kann. Die Verknüpfung von Controllingdaten und Risiken funktioniert. die zur Verfügung stehenden Tools sind brauchbar und erlauben eine Automatisierung der Arbeit.

7 Resultate

In den folgenden Abschnitten werden die Resultate der vorliegenden Arbeit strukturiert dargestellt. Die Resultate beziehen sich einerseits auf die zu beantwortende Hypothese, anderseits auf das erstellte Integrationsmodell für IT-Controlling und IT-Risikomanagement. Zuerst wird die Hypothese in 7.1 beantwortet, dann in 7.2 das vorgestellte Integrationsmodell kritisch beleuchtet.

7.1 Falsifizierung/Verifizierung der Hypothese

Im Folgenden werden die drei Teilthesen der Hypothese beantwortet. Dazu folgt jeweils eine kurze Schlussfolgerung.

7.1.1 (a) Existenz eines Frameworks

Hypothese Teil (a): „Für die Integration von finanziellem und operativem IT-Controlling mit dem IT-Risikomanagement besteht ein geeignetes Framework.“

Aufgrund der in 5.3 gemachten Aussagen muss davon ausgegangen werden, dass zur Zeit kein geeignetes Framework zur Integration von IT-Controlling und Risikomanagement besteht. Die vorgestellten Frameworks und Standards decken höchstens Teilbereiche ab. Den fruchtbarsten Boden für eine Integration bietet aufgrund der in 5.3.2 gemachten Feststellungen der Standard XBRL. Teil (a) kann daher als falsifiziert betrachtet werden.

Schlussfolgerung: Integration betrifft verschiedenste Bereiche einer Organisation. Es ist daher wenig verwunderlich, dass kein Framework besteht, welches sich speziell Integrationsproblemen widmet. Aus diesem Grund wurde versucht mit Extended_XBRL den Ansatz von XBRL weiter zu denken. Einerseits in Richtung der Ausweitung auf das interne Controlling/Risikomanagement. Andererseits auf die

Berücksichtigung nicht technischer Aspekte wie Organisation oder Personal. Extended_XBRL müsste wie in der XBRL Community üblich, in einem zeit- und arbeitsintensiven Prozess entwickelt werden.

7.1.2 (b) Anwendung des Frameworks

Hypothese Teil (b): „Das Framework wird in der Praxis jedoch nicht angewandt.“

In der Praxis wird kaum eines der diskutierten Frameworks durchgängig eingesetzt. Wenn ein Framework wie z.B. ARIS oder ISO 17799 eingesetzt wird, dann nur partiell und nicht mit der expliziten Absicht IT-Controlling und IT-Risikomanagement zusammen zu führen. Diese Aussagen gehen aus den Ausführungen in 4.5 hervor. Teil (b) kann daher als verifiziert betrachtet werden.

Schlussfolgerung: Die unternehmensweite Anwendung nur eines Frameworks lässt sich nicht finden, da jedes Framework nur Teilbedürfnisse befriedigen kann und schwer durchsetzbar ist. Die Durchsetzung von Integrationslösungen und damit von Standards kann wie in 5.1 dargestellt, in seinen Extremformen Softwaretechnisch oder Weisungstechnisch erfolgen. Das auf Basis von XBRL entwickelte Modell Extended_XBRL setzt diese Erkenntnis in die Praxis um. High Level Standards wie CobIT oder ISO 17799 bieten die Durchsetzung durch Beeinflussung der Codierung nicht. Eine XML-basierte Umsetzung bietet jedoch beide Möglichkeiten, die Durchsetzung durch Richtlinien, sowie die Durchsetzung durch Codierung.

7.1.3 (c) Probleme der Umsetzung

Hypothese Teil (c): “Die Probleme bei der Umsetzung liegen hauptsächlich bei den Schnittstellen zwischen den Bereichen, den heterogenen Applikationen, sowie dem vorhandenen Datenmaterial.“

Die in 4.5 gewonnen Informationen legen den Schluss nahe, dass Schnittstellen, sofern sie nicht technisch festgelegt sind, nicht definiert sind. Daraus entstehen zwangsläufig Probleme. Der Einsatz von Applikationen ist sehr heterogen und vielfältig. So werden Excel, Word, SAP, Siebel oder Access parallel und unstrukturiert nebeneinander eingesetzt. Die Kombination von undefinierten Schnittstellen und heterogenen Applikationen erschweren die Verfügbarkeit von relevantem Datenmaterial zur richtigen Zeit am richtigen Ort. Damit zwangsläufig verbunden

sind Probleme bei der Integration von IT-Controlling und IT-Risikomanagement. Teil (c) kann daher als verifiziert betrachtet werden.

Schlussfolgerung: Der Einsatz von heterogenen Applikationen wird auch in Zukunft Realität bleiben und mit der weiter zunehmenden Informatisierung vermehrt zu Schnittstellenproblemen führen. Ohne geeignete Gegenmassnahmen geht mit dieser Entwicklung ein stetiger Effizienzverlust einher. Eine geeignete Gegenmassnahme ist die Anwendung eines Integrationsmodells, hier eines für das IT-Controlling und IT-Risikomanagement. XBRL und Extended_XBRL bieten ein einheitliches Datenmodell und tragen so zur Minimierung von Schnittstellenproblemen bei. Die Basis XML/XBRL/Extended_XBRL ermöglicht den Einsatz verschiedener Applikationen bei gleichem Datenmodell, die Applikationen müssen jedoch über die geeignete Schnittstelle verfügen.

7.2 Kritik des Integrationsmodells

7.2.1 Was gezeigt werden konnte

Der eingeschlagene Weg einer Erweiterung des XBRL Standards hat sich aufgrund der in 5.3.1 durchgeführten Evaluation als der Beste erweisen. Die konkrete Ausgestaltung einer Erweiterung in 5.4 und 5.5 hat gezeigt, dass eine Erweiterung technisch gangbar ist. Die Verifizierung in 6 hat ergeben, dass auch die Anwendung in der Praxis funktioniert.

7.2.2 Lücken und offene Fragen

Trotz der oben erwähnten Punkte bestehen noch Lücken und bleiben offenen Fragen.

Fragmentarischer Charakter des Modells

Die offensichtlichste Lücke ist sicher der fragmentarische Charakter der erstellten XBRL-Erweiterung. Es muss noch viel Arbeit geleistet werden, soll der eingeschlagene Weg auch wirklich zu einem Effizienzgewinn führen.

Lobbying

Innerhalb der XBRL Community muss entsprechendes Lobbying betrieben werden. Es ist nicht zu erwarten, dass die bisher Aktiven der XBRL Community ohne

Einwände einer Erweiterung des Standards zustimmen werden. Einwände könnten in Richtung zunehmender Komplexität oder fehlender Ressourcen gehen.

Fehlende Integration mit XBRL

Ein XML basiertes Framework für das interne Reporting, welches keine Rücksicht auf die bereits bestehende XBRL Taxonomie nimmt ist leichter zu erstellen. Es ist daher zu erwarten, dass XML-Insellösungen erstellt werden. Diese speziell im Hinblick auf Softwareentwicklungsunternehmen, welche oft kein grosses Interesse an offenen Standards haben.

Fehlende Anreize

Das relativ komplizierte Konzept von XML mit seiner Trennung von Daten, Struktur und Darstellung offenbart seine Vorteile nicht sofort. Technisches Know-how ist dazu erforderlich. Weiter ist eine Investition in eine Erweiterung in XBRL eher eine langfristige Investition, welche damit einen unsicheren, zukünftigen Payback aufweist. Damit ist die Anreizproblematik angesprochen. Die Frage, wer Nutzniesser dieser Investition ist, erzeugt weitere Anreizprobleme. Neben der internen Führung haben auch externe Stakeholder wie Aktionäre oder Behörden ein Interesse, einerseits an der Einführung des bestehenden XBRL Standards, anderseits an der hier vorgeschlagenen Erweiterung für das interne Controlling. Der Entscheid über die Investition liegt jedoch zur Zeit ausschliesslich bei der Führung der Firma. Hier könnte externer Druck seitens der betroffenen Stakeholder Abhilfe schaffen.

Nicht existentes IT-Risikomangement

In allen Interviews kam zum Ausdruck, dass keine der befragten Unternehmungen ein explizites Risikomanagement für die IT betreibt, welches über den IT-Grundschutz hinausgeht. Für die Kernkompetenz IT wird das Risikomanagement höchstens innerhalb bestehender Controlling- und Managementstrukturen abgedeckt. Damit ist die Frage einer Integration von IT-Controlling und IT-Risikomanagement vordergründig vom Tisch. Diese Situation trübt den Blick für den Effizienzgewinn einer Integration.

7.3 Handlungsempfehlungen

Die Lücke zwischen Theorie und Praxis soll mittels konkreten Handlungsempfehlungen minimiert werden. Diese sollen der erfolgreichen Integration von IT-Controlling und IT-Risikomanagement dienen.

7.3.1 Prämissen

Die im folgenden erarbeiteten Handlungsempfehlungen gehen von der aktuellen Situation aus, in welcher das skizzierte Integrationsmodell noch zahlreiche Lücken aufweist. Diese Lücken bestehen einerseits bei den Anpassungen innerhalb von XBRL, das heisst in der Definition von Taxonomien, anderseits in den Anpassungen ausserhalb von XBRL, das heisst in der Modellierung von Anforderungen bei Personalfragen, Infrastruktur oder Organisation.

7.3.2 Ziel

Die im folgenden aufgeführten Handlungsempfehlungen haben zum Ziel, eine Integration von IT-Controlling und IT-Risikomanagement mit den bestehenden Integrationsframeworks zum Erfolg zu führen. Der Erfolg soll nachweisbar sein. Als Erfolg wird eine Verbesserung der Wirtschaftlichkeit gewertet. Aber auch eine Beschleunigung der Abläufe oder eine Verbesserung der Qualität kann je nach Situation als Erfolg gewertet werden. Im Endeffekt haben aber sowohl Qualitätsverbesserungen als auch eine Beschleunigung die Verbesserung der Wirtschaftlichkeit zur Folge.

7.3.3 Handlungsempfehlungen oder kritische Erfolgsfaktoren?

Anstelle von Handlungsempfehlungen könnte alternativ auch das bekanntere Konzept der kritischen Erfolgsfaktoren herangezogen werden. Erfolgsfaktoren strahlen allerdings eine gewisse Statik aus. Dies soll hier verhindert werden, vielmehr sollen konkrete, handlungsorientierte und umsetzbare Empfehlungen gegeben werden, *was getan werden muss*, um eine Integration zum Erfolg zu führen.

7.3.4 Handlungsempfehlungen

Die in 5.2 aufgestellten Anforderungen an ein Integrationsmodell für IT-Controlling und IT-Risikomanagement münden in der übergeordneten Anforderung der Wirtschaftlichkeit. Die Wirtschaftlichkeit als Formalanforderung kann jedoch nur

mittels konkreten Sachanforderungen erreicht werden. Die in Abbildung 15 dargestellten sekundären Anforderungen sind diese Sachanforderungen. Handlungsempfehlungen müssen an diesen sekundären Anforderungen anknüpfen. Die folgenden Ausführungen richten sich daher nach den 8 Anforderungsbereichen: Organisation, Mitarbeiter, Tools, Daten, Infrastruktur, Dynamik und Komplexität. Die einzelnen Handlungsempfehlungen in Tabelle 6 sind in eine Einleitung und eine konkrete Handlungsempfehlung (gekennzeichnet mit ☞) gegliedert.

Problembereich	Handlungsempfehlungen
Organisation	Die Einführung eines Integrationsmodells wird stark von der betroffenen Organisationsform beeinflusst. ☞"Bringen Sie deshalb die Integrationsstrategie in Einklang mit der Organisationsform. Eine zentral organisierte Unternehmung erlaubt die Top-Down-Einführung eines Integrationsmodells. Dezentrale geführte Organisationen verlangen ein starkes Projektmarketing."
Mitarbeiter	Wiederstände gegen die Einführung eines Integrationsmodells können aufgrund von sich verschiebenden Machtstrukturen, divergenten Interessen oder aus persönlichen Gründen entstehen. ☞"Machen Sie solche personelle Wiederstände frühestmöglich transparent. Brechen Sie solche Wiederstände durch Commitments, klare Kompetenzallokation oder durch Ausbildung. Nutzen Sie die Möglichkeiten der Durchsetzung mittels Codierung, das heisst Implementieren Sie gewisse Aspekte möglichst früh."
Infrastruktur	Die Einführung eines Integrationsmodells erfordert Investitionen in Infrastruktur. Neuere Infrastruktur ist tendenziell besser für eine Integration geeignet. Allerdings erfüllt auch alte Infrastruktur oft nach kleinen Anpassungen die Integrationsansprüche. ☞"Wägen Sie die mit neuer Infrastruktur verbundenen Kosten, sowohl direkte als auch indirekte, sorgfältig mit den damit verbundenen Nutzen ab."
Daten	Gemäss den Anforderungen an Daten müssen diese verfügbar (intern, extern, technisch, personell und zeitlich), richtig, wirtschaftlich beschaffbar und vertraulich sein. Unklarheiten in der Semantik und der individuelle Einschätzung der Relevanz gefährden die Anforderungen an Daten. ☞"Minimieren Sie Unklarheiten mittels Durchsetzung von geeigneten Datenmodellen. Geeignete Modelle sind XBRL oder Extended_XBRL."
Tools	☞"Stellen Sie sicher, dass unternehmensweit die gleichen Tools eingesetzt werden. Prüfen und validieren Sie die Tools vorgängig."
Dynamik	☞"Wählen Sie das Integrationsmodell so, dass Sie schnell auf regulatorische Änderungen oder veränderte interne Anforderungen reagieren können. Hierzu sind offene Standrads wie XML und XBRL/Extended_XBRL im speziellen geeignet."
Komplexität	Komplexere Fragestellungen im IT-Controlling oder IT-Risikomanagement verleiten schnell dazu, auf bekanntes zurückzugreifen. Das führt nur zu einem Parallelsystem und die geplanten Effizienzsteigerungen bleiben aus. ☞"Verhindern Sie bei komplexen Fragestellungen das Ausweichen auf herkömmliche Verfahren. Schaffen Sie die Voraussetzungen, dass auch komplexe Fragestellungen innerhalb des neuen Integrationsmodells effizienter bearbeitet werden können."

Problembereich	Handlungsempfehlungen
Wirtschaftlichkeit	☞“Verlieren Sie das Oberziel, die Verbesserung der Wirtschaftlichkeit, nie aus den Augen. Messen Sie dazu die Verbesserung der Wirtschaftlichkeit z.B. mittels Key Performace Indicators.“

Tabelle 6: Handlungsempfehlungen erfolgreiche Einführung eines Integrationsmodells

8 Schlussbemerkungen & Ausblick

Eine Standardisierung scheint sowohl im IT-Controlling sowie im IT-Risikomanagement nur schwach ausgeprägt zu sein. Ein Grund liegt dabei auch im schwach ausgeprägten IT-Risikomanagement. Dieses geht selten über den Grundschutz von IT hinaus. Sind Standardisierungen anzutreffen, so handelt es sich dabei meistens um firmeninterne Richtlinien oder die Anwendung von Applikationen, welche gewisse Strukturen vorgeben.

Im externen Reporting geht der XBRL-Ansatz in Richtung unternehmensübergreifender Standardisierung. XBRL wird allerdings erst in wenigen Unternehmen angewandt. Auch der hier vorgeschlagene XML basierte Ansatz für das interne Reporting ist noch in den Kinderschuhen. Die vorgestellte Taxonomie ‚Extended_XBRL’ kann nur Ausgangspunkt für weitere Arbeiten sein. Neben der Erstellung der Taxonomie sind die nicht technischen Anforderungen an ein Integrationsmodell auf keinen Fall aus den Augen zu verlieren.

Es wäre weiter zu prüfen, inwieweit Systemintegratoren oder Anbieter von Standardsoftware firmeninterne Frameworks benutzen.

9 Quick Reference

9.1 Zielpublikum

Die Quick Reference richtet sich an zwei Personengruppen, erstens an Personen welche über die Durchführung von Integrationsprojekten entscheiden, zweitens an Personen welche Integrationsprojekte leiten. Im ersten Fall können das Risikomanager aus der IT, Projektportfoliomanager oder in KMU’s die Geschäftsleitung sein. Im zweiten Fall sind das Projektleiter, Projektmitarbeiter oder betroffene Personen aus dem Business.

9.2 Form

Die Quick Reference ist ein eigenständiges Dokument und soll losgelöst von der vorliegenden Arbeit verstanden werden. Sie hat einen maximalen Umfang von 20 Minuten Studienzeit. Die Quick Reference liegt der Arbeit im Anhang unter 12.2 bei.

9.3 Ziele

Die Quick Reference soll dem Leser die Prinzipien einer XML-basierten Integration von IT-Controlling und IT-Risikomanagement nahe bringen und konkrete Handlungsempfehlungen für eine erfolgreiche Integration geben.

10 Literaturverzeichnis

10.1 Zitierweise

Bücher: [VERWEIS] NACHNAME, VORNAME, TITEL, VERLAG, JAHR
Andere Quellen: [VERWEIS] URL

Alle Angaben zu Onlinequellen beziehen sich auf Anfragen zwischen dem 1. April 2003 und dem 10. Oktober 2003.

10.2 Printquellen

[BORGE01] Borge, Dan, The Book of Risk, Wiley, 2001
[CARR03], Nicholas G. Carr, Harvard Business Review, 1. Mai 2003
[FRÖHLING00] Fröhling, Oliver, KonTraG und Controlling, Verlag Vahlen, 2000
[GYSLER95] Gysler, Thomas P., Informatik-Controlling im Bankbetrieb, Haupt, 1995
[KRCMAR00] Krcmar, Helmut/Burlesch, Alexander/ Reb, Michael, IV-Controlling auf dem Prüfstand, Gabler, 2000
[LESSING00] Lawrence Lessing, Code and Other Laws of Cyberspace, 2000, Basic Books
[PREISSLER98] Preissler Peter R., Controlling, Oldenburg, 1998
[UBSOUTLOOK01] Diverse, UBS Outlook Risikomanagement, UBS AG, Neuauflage 2001
[WEBER02] Weber, Jürgen, Einführng in das Controlling, Schäffer-Poeschel, 2002

[BURGER02] Burger, Anton, Risiko-Controlling, Oldenbourg, 2002

[GAULKE02] Gaulke, Markus, Risikomanagement in IT-Projekten, Oldenbourg, 2002

[HEILMANN01] Heilmann, Heidi, Strategisches IT-Controlling, Hüthig, 2001

[DEMPSTER02] Dempster, M.A.H., Risk management : value at risk and beyond, Cambridge University Press, 2002

[FIGLEWSKI02] Figlewski, Stephen, Risk management : the state of the art, Kluwer Academic, 2002

[STRASSMANN90] Strassmann, Paul A., The Business Value of Computers, Strassmann, 1990

10.3 Elektronische Quellen

[BSI] British Standards Institute, http://www.bsi-global.com

[COBIT] Control Objectives for Information and related Technology, http://www.isaca.org/cobit.htm

[FASB] Financial Accounting Standard Board, http://www.fasb.org/

[GAAP] Generally Generally Accepted Accounting Principles, http://www.fasb.org/

[IDS] IDS Scheer AG, Saarbrücken, http://www.ids-scheer.de/

[INTERVIEWAUFZEICHNUNGEN] Die Interviews liegen grösstenteils als mp3-Files vor. Die Files sind im Anhang aufgeführt und auf CD Nr. 2 enthalten. Die Aufzeichnungen sind für den öffentlichen Zugang gesperrt.

[INTERVIEWTRANSKRIPTE] Von jedem Interview liegt ein Transkript vor. Die Transkripte sind im Anhang enthalten und für den öffentlichen Zugang gesperrt.

[ISACA_RISK] Aus dem FAQ Bereich von http://www.isaca.org/faq_r.htm

[ISACF] Systems Audit and Control Foundation, http://www.isaca.org

[ITIL] http://www.itil-portal.de/

[LEGAMEDIA] http://www.legamedia.net

[W3C] http://www.w3c.org

[XBRL_DEUTSCHLAND] http://www.xbrl-deutschland.de

[XBRL_INTERNATIONAL] http://www.xbrl.org

[XBRL_NEWZEALAND] Mark Hucklesby, Präsentation vom 2. August 2002

[XMLGLOBAL] http://www.xmlglobal.com/

[XMLSPY] XMLSPY Enterprise Edition Version 5, http://www.altova.com

11 Abbildungen, Formeln & Tabellen

12 Anhang

12.1 XML Files

12.1.1 Schema

Das File (Extended_XBRL.xsd) liegt auch auf der beiliegenden CD Nr. 1 vor.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- edited with XMLSPY v5 rel. 4 U (http://www.xmlspy.com) by Daniel M. Schmid, 28.Aug.2003 -->
<xs:schema targetNamespace="http://www.danielschmid.com/Extended_XBRL"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns="http://www.danielschmid.com/Extended_XBRL"
elementFormDefault="qualified">
    <xs:element name="IntegratedObject">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="ControllingObject" maxOccurs="unbounded">
                    <xs:complexType>
                        <xs:sequence>
                            <xs:element name="ObjectInformation">
                                <xs:complexType>
                                    <xs:sequence>
```

```
                        <xs:element name="ObjectID" type="xs:string"/>
                        <xs:element name="Name" type="xs:string"/>
                        <xs:element name="Description"/>
                        <xs:element name="PeriodStart" type="xs:string"/>
                        <xs:element name="PeriodEnd" type="xs:string"/>
                        <xs:element name="Responsable" type="xs:string"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="BudgetControl">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element name="BudgetControlID" type="xs:string"/>
                        <xs:element name="Description"/>
                        <xs:element name="Plan" type="xs:string"/>
                        <xs:element name="Achieved" type="xs:string"/>
                        <xs:element name="DeviationPlanMinusAchieved" type="xs:string"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="ProgressControl">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element name="ProgressControlID" type="xs:string"/>
                        <xs:element name="Description"/>
                        <xs:element name="Plan" type="xs:string"/>
                        <xs:element name="Achieved" type="xs:string"/>
                        <xs:element name="DeviationPlanMinusAchieved" type="xs:string"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="RessourceControl">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element name="RessourceControlID" type="xs:string"/>
                        <xs:element name="Description"/>
                        <xs:element name="Plan" type="xs:string"/>
                        <xs:element name="Achieved" type="xs:string"/>
                        <xs:element name="DeviationPlanMinusAchieved" type="xs:string"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="TimeControl">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element name="TimeControlID" type="xs:string"/>
                        <xs:element name="Description"/>
                        <xs:element name="Plan" type="xs:string"/>
                        <xs:element name="Achieved" type="xs:string"/>
                        <xs:element name="DeviationPlanMinusAchieved" type="xs:string"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="QualityControl">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element name="QualityControlID" type="xs:string"/>
                        <xs:element name="Description"/>
                        <xs:element name="Plan" type="xs:string"/>
                        <xs:element name="Achieved" type="xs:string"/>
                        <xs:element name="DeviationPlanMinusAchieved" type="xs:string"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
        </xs:sequence>
    </xs:complexType>
</xs:element>
<xs:element name="RiskObject" maxOccurs="unbounded">
    <xs:complexType>
        <xs:sequence>
            <xs:element name="ObjectInformation">
```

```
                        <xs:complexType>
                            <xs:sequence>
                                <xs:element name="ObjectID" type="xs:string"/>
                                <xs:element name="Name" type="xs:string"/>
                                <xs:element name="AssessedPeriodStart" type="xs:string"/>
                                <xs:element name="AssessedPeriodEnd" type="xs:string"/>
                                <xs:element name="Responsable" type="xs:string"/>
                            </xs:sequence>
                        </xs:complexType>
                    </xs:element>
                    <xs:element name="ReferenceToControl">
                        <xs:complexType>
                            <xs:sequence>
                                <xs:element name="ReferenceToControlID" type="xs:string"/>
                                <xs:element name="ReferenceDescription" type="xs:string"/>
                                <xs:element name="ReferenceFormula" type="xs:string"/>
                            </xs:sequence>
                        </xs:complexType>
                    </xs:element>
                    <xs:element name="ReferenceToRisk">
                        <xs:complexType>
                            <xs:sequence>
                                <xs:element name="ReferenceToRiskID" type="xs:string"/>
                                <xs:element name="ReferenceDescription" type="xs:string"/>
                                <xs:element name="ReferenceFormula" type="xs:string"/>
                            </xs:sequence>
                        </xs:complexType>
                    </xs:element>
                    <xs:element name="Impact">
                        <xs:complexType>
                            <xs:sequence>
                                <xs:element name="Description" type="xs:string"/>
                                <xs:element name="ExpectationValue" type="xs:string"/>
                            </xs:sequence>
                        </xs:complexType>
                    </xs:element>
                    <xs:element name="Probability">
                        <xs:complexType>
                            <xs:sequence>
                                <xs:element name="Distribution" type="xs:string"/>
                                <xs:element name="DistributionParmeters" type="xs:string"/>
                            </xs:sequence>
                        </xs:complexType>
                    </xs:element>
                </xs:sequence>
            </xs:complexType>
        </xs:element>
    </xs:sequence>
  </xs:complexType>
 </xs:element>
</xs:schema>
```

12.1.2 Instanzdokument

Das File (Extended_XBRL_Instance.xml) liegt auch auf der beiliegenden CD Nr. 1 vor.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- edited with XMLSPY v5 rel. 4 U (http://www.xmlspy.com) by Daniel M. Schmid, 28.Aug.2003 -->
<IntegratedObject xmlns="http://www.danielschmid.com/Extended_XBRL"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.danielschmid.com/Extended_XBRL
C:\DOCUME~1\Administrator\Desktop\Extended_XBRL.xsd">
    <ControllingObject>
        <ObjectInformation>
            <ObjectID>C0010</ObjectID>
            <Name>SAP-Einfuehrung</Name>
            <Description>Projektcontrolling SAP-Einführung</Description>
            <PeriodStart>01.07.02</PeriodStart>
```

```
            <PeriodEnd>31.07.03</PeriodEnd>
            <Responsable>Daniel M. Schmid</Responsable>
        </ObjectInformation>
        <BudgetControl>
            <BudgetControlID>C0011</BudgetControlID>
            <Description>Budgetzahlen des Gesamtprojektes in CHF</Description>
            <Plan>104000</Plan>
            <Achieved>120000</Achieved>
            <DeviationPlanMinusAchieved>-16000</DeviationPlanMinusAchieved>
        </BudgetControl>
        <ProgressControl>
            <ProgressControlID>C0012</ProgressControlID>
            <Description>Anzahl abgenommener Funktionen vom Fachdienst</Description>
            <Plan>10</Plan>
            <Achieved>8</Achieved>
            <DeviationPlanMinusAchieved>2</DeviationPlanMinusAchieved>
        </ProgressControl>
        <RessourceControl>
            <RessourceControlID>C0013</RessourceControlID>
            <Description>Auslastung des Projektteams</Description>
            <Plan>100%</Plan>
            <Achieved>110%</Achieved>
            <DeviationPlanMinusAchieved>-10%</DeviationPlanMinusAchieved>
        </RessourceControl>
        <TimeControl>
            <TimeControlID>C0014</TimeControlID>
            <Description>Anzahl erreichter Meilensteine</Description>
            <Plan>2</Plan>
            <Achieved>1</Achieved>
            <DeviationPlanMinusAchieved>1</DeviationPlanMinusAchieved>
        </TimeControl>
        <QualityControl>
            <QualityControlID>C0015</QualityControlID>
            <Description>ANzahl neuer Störrapporte</Description>
            <Plan>0</Plan>
            <Achieved>5</Achieved>
            <DeviationPlanMinusAchieved>-5</DeviationPlanMinusAchieved>
        </QualityControl>
    </ControllingObject>
    <RiskObject>
        <ObjectInformation>
            <ObjectID>R0001</ObjectID>
            <Name>Budgetüberschreitung</Name>
            <AssessedPeriodStart>01.08.02</AssessedPeriodStart>
            <AssessedPeriodEnd>31.10.02</AssessedPeriodEnd>
            <Responsable>Daniel M. Schmid</Responsable>
        </ObjectInformation>
        <ReferenceToControl>
            <ReferenceToControlID>C0011</ReferenceToControlID>
            <ReferenceDescription>Das Risiko der Budegtueberschreitung ist direkt abhängig vom Mehrverbrauch an
            Mitteln</ReferenceDescription>
            <ReferenceFormula>8xAbweichung vom Budget</ReferenceFormula>
        </ReferenceToControl>
        <ReferenceToRisk>
            <ReferenceToRiskID>none</ReferenceToRiskID>
            <ReferenceDescription>none</ReferenceDescription>
            <ReferenceFormula>none</ReferenceFormula>
        </ReferenceToRisk>
        <Impact>
            <Description>Aufgrund einer aktuellen Budgetueberschreitung kann auf wahrscheinliche, zukuenftige
            Budgetueberschreitungen geschlossen werden.</Description>
            <ExpectationValue>-80000</ExpectationValue>
        </Impact>
        <Probability>
            <Distribution>Dreiecksverteilung</Distribution>
            <DistributionParmeters>a=-80000, b=0</DistributionParmeters>
        </Probability>
    </RiskObject>
    <RiskObject>
        <ObjectInformation>
            <ObjectID>R0002</ObjectID>
```

```
            <Name>Personalueberlastung</Name>
            <AssessedPeriodStart>01.08.02</AssessedPeriodStart>
            <AssessedPeriodEnd>31.10.02</AssessedPeriodEnd>
            <Responsable>Daniel M. Schmid</Responsable>
        </ObjectInformation>
        <ReferenceToControl>
            <ReferenceToControlID>C0013</ReferenceToControlID>
            <ReferenceDescription>Personalüberlastung stellt an sich ein Risiko dar.</ReferenceDescription>
            <ReferenceFormula>none</ReferenceFormula>
        </ReferenceToControl>
        <ReferenceToRisk>
            <ReferenceToRiskID>none</ReferenceToRiskID>
            <ReferenceDescription>none</ReferenceDescription>
            <ReferenceFormula>none</ReferenceFormula>
        </ReferenceToRisk>
        <Impact>
            <Description>Personalüberlastungen führen zu Personalproblemene und einer Verzögerung im
            Einführungstermin. Jeder Monat zu später Einführung kosten zusätzlche Projektkosten sowie Betriebskosten
            der Altsystemem. Entgangene Vorteile im Business sind nicht enthalten.</Description>
            <ExpectationValue>-150000</ExpectationValue>
        </Impact>
        <Probability>
            <Distribution>Normalverteilung</Distribution>
            <DistributionParmeters>μ=-150000, σ=100000</DistributionParmeters>
        </Probability>
    </RiskObject>
    <RiskObject>
        <ObjectInformation>
            <ObjectID>R0003</ObjectID>
            <Name>Verspaetete Einführung</Name>
            <AssessedPeriodStart>01.08.02</AssessedPeriodStart>
            <AssessedPeriodEnd>31.10.03</AssessedPeriodEnd>
            <Responsable>Daniel M. Schmid</Responsable>
        </ObjectInformation>
        <ReferenceToControl>
            <ReferenceToControlID>none</ReferenceToControlID>
            <ReferenceDescription>none</ReferenceDescription>
            <ReferenceFormula>none</ReferenceFormula>
        </ReferenceToControl>
        <ReferenceToRisk>
            <ReferenceToRiskID>R0002</ReferenceToRiskID>
            <ReferenceDescription>Personalüberlastng ist ein wichtiger Einflussfaktor für verspätete
            Einführung</ReferenceDescription>
            <ReferenceFormula>none</ReferenceFormula>
        </ReferenceToRisk>
        <Impact>
            <Description>Neben der Personalüberlastung führen auch noch extere Faktoren wie Supportverhalten von
            SAP oder GL-Entscheide zu Verzögerungen massgeblich bei.</Description>
            <ExpectationValue>-200000</ExpectationValue>
        </Impact>
        <Probability>
            <Distribution>Chi-Quadrat-Verteilung</Distribution>
            <DistributionParmeters>n=200000</DistributionParmeters>
        </Probability>
    </RiskObject>
    <RiskObject>
        <ObjectInformation>
            <ObjectID>R0004</ObjectID>
            <Name>Stabilitätsprobleme</Name>
            <AssessedPeriodStart>01.08.03</AssessedPeriodStart>
            <AssessedPeriodEnd>31.10.02</AssessedPeriodEnd>
            <Responsable>Daniel M. Schmid</Responsable>
        </ObjectInformation>
        <ReferenceToControl>
            <ReferenceToControlID>C0015</ReferenceToControlID>
            <ReferenceDescription>Das nicht Erreichen von Qualitätskriterien hat STabilitätsprobleme der Aplikation zur
            Folge</ReferenceDescription>
            <ReferenceFormula>Abweichung x 50000</ReferenceFormula>
        </ReferenceToControl>
        <ReferenceToRisk>
            <ReferenceToRiskID>String</ReferenceToRiskID>
```

```
            <ReferenceDescription>String</ReferenceDescription>
            <ReferenceFormula>none</ReferenceFormula>
        </ReferenceToRisk>
        <Impact>
            <Description>Stabilitätsprobleme durch Qualitätsmängel verursachen Kosten im Business sowie in erhöhten
            Wartungskosten.</Description>
            <ExpectationValue>-250000</ExpectationValue>
        </Impact>
        <Probability>
            <Distribution>Normalverteilung</Distribution>
            <DistributionParmeters>μ=-250000, σ=150000</DistributionParmeters>
        </Probability>
    </RiskObject>
</IntegratedObject>
```

12.2 Quick Reference

Quick Reference

Erfolgreiche Integration von IT-Controlling & IT-Risikomanagement

Die Quick Reference ist Bestandteil der Diplomarbeit „Integration von finanziellem und operativem IT-Controlling mit dem IT-Risikomanagement: Konzepte und praktische Umsetzung“ von Daniel M. Schmid, IFI, Universität Zürich, 2003

Kontakt: schmid.dani@gmx.net

Grundlagen Ziele

Die vorliegende Quick Reference präsentiert wichtige Grundlagen einer XML-basierten Integration von IT-Controlling und IT-Risikomanagement und gibt konkrete Handlungsempfehlungen für eine erfolgreiche Umsetzung ab.

Vorbild ist die Darstellung externer Reportingdaten in XBRL (Extended Busines Reporting Language, ein XML Dialekt). Nach dem gleichen Prinzip können interne Daten aus IT-Controlling und IT-Risikomanagement in Exteded_XBRL dargestellt werden. XBRL ist voll entwickelt, Extended_XBRL ist erst in Ansätzen vorhanden. Eine Architekturübersicht gibt Abbildung 1.

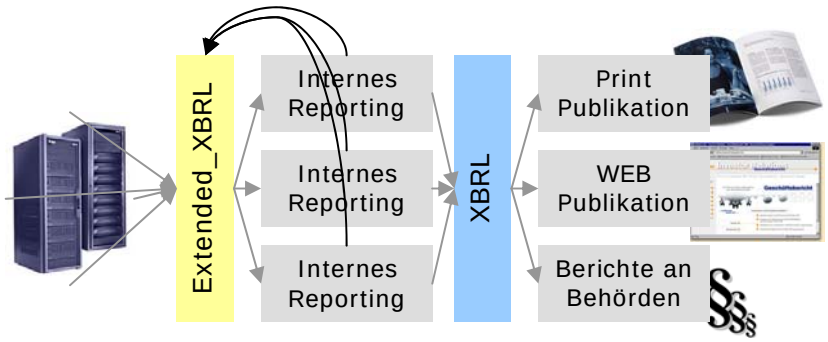

Abbildung 1: Extended_XBRL Architektur

Das integrierte Datenmodell in Extended_XBRL erlaubt die Verlinkung von IT-Controllingdaten mit IT-Risiken. Risiken werden dabei als eigenständig oder als Folge von Kontrollabweichungen modelliert. Abbildung 2 visualisiert das Datenmodell.

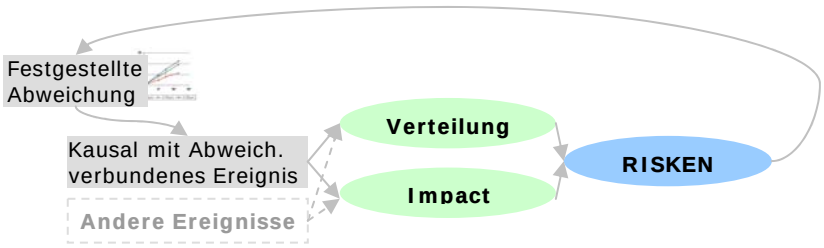

Abbildung 2: Zusammenhang Controlling & Risiko

An oberster Stelle der Anforderungen an eine Integration steht die Wirtschaftlichkeit.
Alle anderen Anforderungen sind der Wirtschaftlichkeit untergeordnet, haben auf diese aber Einfluss. Die Wirtschaftlichkeit kann nur über die untergeordneten, sekundären Anforderungen beeinflusst werden. Abbildung 3 gibt eine Übersicht über die acht Anforderungsbereiche.

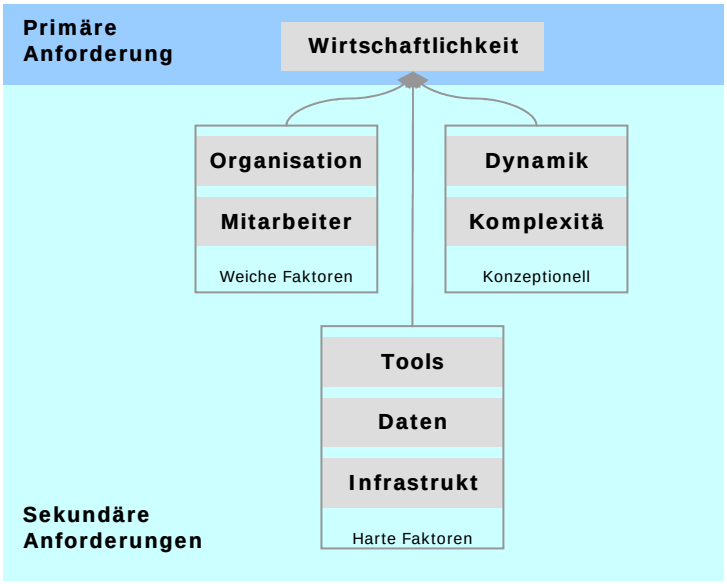

Abbildung 3: Anforderungen an ein Integrationskonzept

Basierend auf dem Schema in Abbildung 3 werden im folgenden konkrete Handlungsempfehlungen für alle acht Anforderungsbereiche abgegeben.

Handlungsempfehlungen

In Tabelle 1 sind konkrete Handlungsempfehlungen für ein Integrationsprojekt aufgeführt. Diese zielen primär auf die Einführung von Extended_XBRL ab, können aber auch allgemein z.B. für die Einführung von XBRL oder einer eigenen Integrationslösung herangezogen werden.

Problembereich	Handlungsempfehlung
Organisation	☞"Bringen Sie die Integrationsstrategie in Einklang mit der Organisationsform. Eine zentral organisierte Unternehmung erlaubt die Top-Down-Einführung eines Integrationsmodells. Dezentrale geführte Organisationen verlangen ein starkes Projektmarketing."
Mitarbeiter	☞"Machen Sie personelle Wiederstände frühestmöglich transparent. Brechen Sie solche Wiederstände durch Commitments, klare Kompetenzallokation oder durch Ausbildung. Nutzen Sie die Möglichkeiten der Durchsetzung mittels Codierung, das heisst Implementieren Sie gewisse Aspekte möglichst früh."
Infrastruktur	☞"Wägen Sie die mit neuer Infrastruktur verbundenen Kosten, sowohl direkte als auch indirekte, sorgfältig mit den damit verbundenen Nutzen ab."
Daten	☞"Minimieren Sie Unklarheiten mittels Durchsetzung von geeigneten Datenmodellen. Geeignete Modelle sind XBRL oder Extended_XBRL."
Tools	☞"Stellen Sie sicher, dass unternehmensweit die gleichen Tools eingesetzt werden. Prüfen und validieren Sie die Tools vorgängig."
Dynamik	☞"Wählen Sie das Integrationsmodell so, dass Sie schnell auf regulatorische Änderungen oder veränderte interne Anforderungen reagieren können. Hierzu sind offene Standrads wie XML und XBRL/Extended_XBRL im speziellen geeignet."
Komplexität	☞"Verhindern Sie bei komplexen Fragestellungen, dass Ausweichen auf herkömmliche Verfahren. Schaffen Sie die Voraussetzungen, dass auch komplexe Fragestellungen innerhalb des neuen Integrationsmodells effizienter bearbeitet werden können."
Wirtschaftlichkeit	☞"Verlieren Sie das Oberziel, die Verbesserung der Wirtschaftlichkeit nie aus den Augen. Messen Sie dazu die Verbesserung der Wirtschaftlichkeit z.B. mittels Key Performace Indicators."

Tabelle 1: Handlungsempfehlungen

13 Anhang (Sperrvermerk)

13.1 Interviewtranskripte

Die Interviewtranskripte sind nicht Bestandteil der öffentlichen Version.

13.2 Audiofiles der Interviews

Die Audiofiles sind nicht Bestandteil der öffentlichen Version.