TECHNISCHE UNIVERSITÄT WIEN
Vienna University of Technology

Unternehmensweites Risikomanagement - Systemdesign und prototypische Implementierung

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des Studiums

Wirtschaftsingenieurwesen - Maschinenbau

eingereicht von

Martin Marenich, BSc
Matrikelnummer 0525360

an der
Fakultät für Maschinenwesen und Betriebswissenschaften der Technischen Universität Wien

Betreuung
Betreuer: Univ. Prof. Mag. rer. soc. oec. Dr. rer. soc. oec. Walter Schwaiger, MBA

Wien, 24.01.2016 _____ _____

(Unterschrift Verfasser) (Unterschrift Betreuer)

TECHNISCHE
UNIVERSITÄT
WIEN
Vienna University of Technology

Ich habe zur Kenntnis genommen, dass ich zur Drucklegung meiner Arbeit unter der Bezeichnung

DIPLOMARBEIT

nur mit Bewilligung der Prüfungskommission berechtigt bin.

Ich erkläre weiters an Eides statt, dass ich meine Diplomarbeit nach den anerkannten Grundsätzen für wissenschaftliche Abhandlungen selbständig ausgeführt habe und alle verwendeten Hilfsmittel, insbesondere die zugrunde gelegte Literatur genannt habe.

Weiters erkläre ich, dass ich dieses Diplomarbeitsthema bisher weder im In- noch im Ausland einer Beurteilerin/einem Beurteiler zur Begutachtung in irgendeiner Form als Prüfungsarbeit vorgelegt habe und dass diese Arbeit mit der vom Begutachter beurteilten Arbeit übereinstimmt.

Wien, am 24. Jänner 2016 .....
(Martin Marenich)

Danksagung

Zuerst möchte ich mich bei allen Personen bedanken, die diese Arbeit unterstützt haben. Sie ist das Ergebnis meines 18-monatigen Forschungsprojekts mit Prof. Schwaiger, der Ottakringer Getränke AG und prevero AG. Allen MitarbeiterInnen dieser Organisationen möchte ich herzlich für ihre freundliche und offene Aufnahme danken.

Ein besonderer Dank gilt Herrn Univ. Prof. Schwaiger für die hervorragende Betreuung bei der Durchführung dieser Diplomarbeit. Im Zuge dutzender Besprechungen hatte ich die Möglichkeit mit Ihm über sinnvolles Risikomanagement zu diskutieren.

Im Zuge der rund 25 Workshops und Besprechungen in der Ottakringer Getränke AG waren Dr. Barbara Weinwurm, DI. Johann Grameder und Mag. Christoph Aichinger die denkbar besten und motiviertesten Kollegen. Sie haben einen Riesenanteil am gelingen dieser Arbeit, vielen Dank!

Bei der prevero AG wurde während mehrerer, geduldiger Entwicklungstage der Prototyp entwickelt. Dies wäre ohne die Unterstützung des Entwicklers Edin Cizmic und der beiden Vorstände DI. Matthias Thurner und Mag. Alexander Hain, nicht möglich gewesen, Dankeschön!

Der größte Dank gebührt meiner Familie. Vor allem meinen Eltern Karin und Johann, die mir mein Studium ermöglichten und immer voller Unterstützung für mich da waren. Meiner Schwester Margit für das Korrekturlesen der Arbeit und meiner Partnerin Isabella, die mir immer mit viel Motivation zur Seite stand.

Diese Diplomarbeit zeigt die Ergebnisse meiner Entdeckungsreise durch die Welt des Risikomanagements. Die vielen Begegnungen und der Erfahrungsaustausch ermöglichten einen tiefen Einblick in die Realität von Theorie und Praxis, Dank für ihre Zeit und Erfahrungen gebühren:

Werner Aschenberger (KTM), Dr. Brugger (dbj Rechtsanwälte), Prof. Thomas Dangl (TU Wien), Prof. Paul Embrechts - (ETH Zürich), Bernhard Hirsch (OenB), Dr. Hubert Figl (RZB), Walter Gries (Thomson Reuters GRC), Andreas Gödde (SAS Institute), Emmanuel Hahn (Plasser & Theurer GmbH), Mag. Beata Hartl (RZB), Martin Heiss (A1 Telekom), Daniel Holzinger (avedos business solutions), Prof. Friedrich Hubalek (TU Wien), Dr. Kronfellner (BCG), DI. Benedikt Schraik (pwc Strategy&), Ralf Kimpel (Burda Media Holding), Prof. Josef Kreiner (TU Graz), Veronika Lanka (RZB), Dr. Peter Lechner (Raiffeisen Bausparkasse), Dr. Thomas Lederer (MISYS), DI. Andreas Kopper (McKinsey), Klaus Paier (Firma Rondo Ganahl), Alina Cristina Popescu (OMV), Oliver Hrazdera (Rosensteiner), Dr. Christoph Ruth (accenture), DI. Andreas Schleinzer (BOC), Dr. Alexander Schloske (Fraunhofer), Adam Schnellbach (Magna), Bernhard Schussek (open-souce Entwickler), Prof. Gernot Tragler (TU Wien), DI. Roland Ulbricht (accenture) und Dr. Karl Wagner (procon).

Diese Arbeit über Risikomanagement wollte klären, was die Wissenschaft kann, was der Gesetzgeber will und was die Unternehmen schaffen. Eines ist vor allen anderen Dingen klar: Es gibt noch genug Stoff für viele andere Forschungs-, und Diplomarbeiten.

Wien, am 24. Jänner 2016 Martin Marenich

Zusammenfassung

Risikomanagement ist zu einem unverzichtbaren Teil in der heutigen Unternehmensrealität geworden. Krisen verschiedenster Art sowie spektakuläre Unternehmenspleiten führten in den letzten Jahren zu einem Bedeutungszuwachs des Risikomanagements, sowohl in der gelebten Unternehmenspraxis als auch im regulatorischen Bewusstsein.

Dabei ist eine Neupositionierung weg vom traditionellen ex-post Compliance- und Kontrollzugang hin zu einem auf allen Unternehmensebenen integrierten Bestandteil zu beobachten. Unternehmen sind zunehmend gefordert Risiko systematisch, ganzheitlich und vor allem ex-ante, also vorausschauend, anzugehen, um bewusst das Eingehen von Risiken und deren Chancen zu managen.

Im Zuge dieser Arbeit wird anhand von konkreten Anforderungen eines mittelständischen Industriekonzerns ein unternehmensweites und softwareunterstütztes Risikomanagementsystem entwickelt. Die Ermittlung des aktuellen Industriestandards, der gesetzlichen Mindestanforderungen und der nötigen Funktionen eines softwareunterstütztes Informationssystem stehen dabei im Vordergrund. Die als Grundlage verwendete Theorie orientiert sich an dem regelkreisgesteuerten Risikomanagementansatz, wie er im enterprise-risk-management-framework von COSO II und in der ISO 31000 Norm beschrieben wird.

Die Ergebnisse dieser Arbeit helfen mittelständischen Industrieunternehmen bei der Einführung eines für sie passenden Risikomanagementsystems, da sie in der Regel dabei Schwierigkeiten haben. Dies ist begründet durch die Fülle an Varianten, Literatur, Regelwerken, Methoden, Kennzahlen und Gesetzen, sowie gleichzeitig durch die Abwesenheit eines eindeutigen best-practice Ansatzes.

Die vorliegende Arbeit zeigt, dass ein Risikomanagementsystem erst seinen vollen Nutzen entfaltet, wenn erstens die Konzeption speziell auf das Unternehmen angepasst ist, es zweitens parallel in ein softwareunterstützendes Informationssystem eingebettet wird und drittens durch einen proaktiven Risikomanagementansatz auch die Chancen, die sich ergeben können, gezielt genutzt werden.

Zusätzlich umfasst der wissenschaftliche Mehrwert dieser Arbeit ein Modell zur Risikokategorisierung inklusive Risikokontorahmen; eine Risikopyramide, die das strategische Risikomanagement mit der Risikokalkulation verbindet; eine mittelständische Organisationsstruktur; ein umfangreiches Reifegradmodell; eine einfache Risikoberechnung in Form von Quantifizierung und Aggregation mittels Risikolandkarten; ein Anwendungsleitfaden in Form eines Handbuchs; ein Risikomanagement-Datenmodell und die Gestaltung der Benutzeroberfläche als übersichtliche Workflow und Managementcockpits.

Abschließend kann gesagt werden, dass die naturwissenschaftlichen Methoden erstaunlich wenig zum beiliegenden Projekt beitragen konnten. Es sind vielmehr Softskills von Risikokultur bis hin zu Transparenz und die Aufbereitung und Auswertung von Informationen, die wesentlich für den Erfolg eines Risikomanagementsystems verantwortlich sind. Und genau diese weichen Faktoren bieten weitere Forschungsmöglichkeiten für empirische Studien oder Modellentwicklungen, die das Risikomanagement besser im Unternehmen verknüpfen können. Trotzdem sollte weiterhin nach einem akzeptablem Modell aus technischen und mathematischen Methoden geforscht werden, nach dem Motto “so wenig wie möglich und so viel wie nötig”.

Abstract

In today's world, risk management has evolved to an inevitable component enterprises must not ignore any more. During the past decades various crises (e.g. spectacular bankruptcy or fraud cases) led to both, an increasing importance of enterprise-wide risk management and an ever growing regulatory framework.

Within risk management, a paradigm change occurred during this period, away from the ex-post view as a controlling tool towards an active involvement throughout the whole spectrum of company activities. This new risk management philosophy increasingly requires enterprises to tackle risks ex-ante from a 360° perspective and to decide beforehand what chances and risks the company should take or not take.

In this thesis specific requirements for a software-supported risk management platform are developed, in consideration of industrial small-medium-enterprise (SME) needs. Therefore prior investigation of the current industry standard, regulatory minimal requirements and necessary functionality are conducted.

Based on these considerations, the risk management processes of COSO II ERM and ISO 31000 are used as basic frameworks for this thesis.

The results of this thesis are intended to help industrial SMEs implementing a suitable risk management platform, which is often a difficult task due to the vast amount of literature, frameworks, methods, key performance indicators, laws and especially the lack of general best practice cases.

In general, a risk management platform only unfolds its full potential when:

1. The concept is tailored to the traditions and processes of the specific company.
2. In parallel a software-based information system is embedded with the risk management.
3. A proactive risk management approach targets the potential chances as well as the involved risk.

The first and second points are the main focus of this thesis.

The scientific output and added value of this thesis include a numbered risk categorisation; a so-called risk pyramid, where the strategic risk management is connected to the calculation; a proposed organisational hierarchy; an extensive risk management maturity model; a sound quantitative risk calculation and aggregation by means of risk maps; a comprehensive risk management handbook; an entity-relation-diagram for risk management as well as designed user-interfaces, management cockpits and workflows.

In conclusion, it is apparent that scientific and statistical methods contributed astonishingly little to the successful risk management implementation project conducted in this thesis. Instead, soft skills (ranging from a positive risk culture to a transparent work environment and the information collection and analysis) have been most beneficial. These soft skills provide many future research opportunities, for example the optimum way of anchoring risk management within the whole company. Nevertheless, this does not necessarily exclude research on scientific and statistical methods which should be further enhanced.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Teil I

Das Risiko in der Welt von Heute

KAPITEL 1

Einleitung

1.1 Motivation und Rahmenbedingungen

> "Nach Peter Drucker gibt es vier Risikoarten, erstens die es zu akzeptieren gilt, da sie Bestandteil der Tätigkeit sind, jene die zu vermeiden möglich sind, drittens Risiken, die einzugehen man sich nicht leisten darf und letztens Risiken die nicht einzugehen, man sich nicht leisten darf" [Drucker(1964), S.193].

Risikomanagement ist ein unverzichtbarer Teil eines heutigen Unternehmens geworden. Krisen verschiedenster Art, sowie spektakuläre Unternehmenspleiten führten in den letzten Jahren zu einem Bedeutungszuwachs, sowohl in der gelebten Unternehmenspraxis als auch im regulatorischen Bewusstsein.

> "Im heutigen Geschäftsalltag ist Risiko zentraler Bestandteil aller Tätigkeiten eines Unternehmens. Risiken treten auf der operativen Prozessebene, der finanziellen Geschäftsebene und der strategischen Unternehmensebene in Erscheinung. Dabei zeigen sich die Risiken in verschiedenen Varianten, und die verschiedenen Risikoarten erfordern auch unterschiedliche Managementmethoden. Die Vielfalt an Risikoarten und Managementmethoden erfordert einen systematischen Zugang, um die Risiken des Unternehmens gesamthaft unter Kontrolle zu bringen." [Schwaiger(2013)].

Diese Entwicklung schreitet zudem weiterhin rasant voran. So beobachteten Beratungsunternehmen [1] eine Verschiebung, weg vom traditionellen Compliance- und Kontrollzugang, hin zu einem auf allen Unternehmensebenen integrierten Bestandteil. Dies bedeutet de facto eine klare Aufwertung sowie eine Neupositionierung des Risikomanagements.

[1] vgl. [accenture(2011)], [Plaschke et al.(2013)Plaschke, Rodt, Pidun, and Günther] oder [McNish(März 2013)].

Unternehmen haben jedoch Schwierigkeiten bei der Einführung eines für sie passenden Risikomanagementsystems. Dies ist begründet durch die Fülle an Varianten, Literatur, Regelwerken, Methoden, Kennzahlen und Gesetzen, sowie gleichzeitig durch die Abwesenheit eines eindeutigen best-practice Ansatzes.

Außerdem entfaltet ein Risikomanagementsystem erst seinen vollen Nutzen, wenn erstens die Konzeption speziell auf das Unternehmen angepasst ist, es zweitens parallel in ein softwareunterstützendes Informationssystem eingebettet wird und drittens durch einen proaktiven Risikomanagementansatz auch die Chancen, die sich ergeben können, gezielt genutzt werden. Die ersten beiden Punkte sind die Schwerpunkte dieser Arbeit.

1.2 Ziele der Arbeit

Ziel dieser Arbeit ist es, anhand von konkreten Anforderungen eines mittelständischen Industriekonzerns ein unternehmensweites und softwareunterstütztes Risikomanagementsystem zu entwickeln.

Die folgenden Teilziele sollen im Zuge eines Forschungsprojekts in Zusammenarbeit zwischen dem Institut für Managementwissenschaften, der Ottakringer Getränke AG und der prevero AG geklärt werden:

1. Ermittlung des aktuellen Industriestandards und der gesetzlichen Mindestanforderungen im Hinblick auf Risikomanagement
2. Entwicklung eines unternehmensweiten und regelkreisgesteuerten Risikomanagementsystems ausgehend von den Bedürfnissen eines mittelständischen Industriekonzerns.
3. Einführung eines normgerechten Risikomanagementsystems in einem mittelständischen Industrieunternehmen
4. Weiterentwicklung des Risikomanagements durch ein softwareunterstütztes Informationssystem

Die Arbeit kann in zwei grobe Themenstellungen unterteilt werden, wobei das Risikomanagementsystem die Teilziele 1, 2 und 3 und das softwareunterstützte Informationssystem die Teilziele 1 und 4 betrifft.

1.3 Verwendete Methodik

Die Entwicklung orientiert sich an dem regelkreisgesteuerten Risikomanagementansatz, wie er im enterprise-risk-management-framework von COSO II und in der ISO 31000 Norm beschrieben wird. Folgende Methoden werden für die Erreichung der einzelnen Teilziele eingesetzt:

- Einleitend wird eine umfangreiche Recherche zum Thema Risikomanagementsysteme unternommen. Es sollen wissenschaftliche Erkenntnisse und gängige Methoden

aus der Praxis ermittelt werden. Die daraus resultierende umfassende Sichtweise soll die praktischen Entwicklungsentscheidungen unterstützen.

- Eine wissenschaftliche Begleitung während der kompletten Projekteinführung im Partnerunternehmen soll den Ist- und Sollzustand der Unternehmenspraxis aus internen Workshops und Befragungen ermitteln. Insbesondere sind die realen Zustände der Prozesse, Datenquellen, Methoden und Organisationsstrukturen in Erfahrung zu bringen.

- Auf Basis der Anforderungen aus Literaturrecherche und COSO II / ISO 31000 Normen einerseits und praktischen Erkenntnissen andererseits, soll ein generischer Prototyp als Microsoft Excel mock-up aufgebaut und im Unternehmen getestet werden.

- Eine zweite Literaturrecherche inklusive case studies aus ausgewählten Unternehmen zum Thema analytisches Informationssystem sollen deren modernen Aufbau und Implementierung ermöglichen.

- Anhand der Vorgaben der zweiten Literaturrecherche und von Testergebnissen des ersten Prototyps wird ein zweiter Prototyp als Risikomodul des bestehenden analytischen Informationssystems “prevero p7 maple leaf” entwickelt. Im Zuge der Entwicklungsmethode Prototyping soll fortlaufend der Prototyp mit Rückmeldungen und Daten aus dem Unternehmen ergänzt und getestet werden. Dadurch soll die Erfüllung der Unternehmensbedürfnisse sichergestellt werden.

- Die Präsentation der Prototypen und des Risikomanagementhandbuchs bilden die abschließende Evaluierung des Projekts mit den Forschungspartnern.

KAPITEL 2

Risikomanagement Grundlagen

Zur Klärung des Industriestandards beschäftigt sich dieses Kapitel mit der Geschichte des Risikos, insbesondere in Bezug auf Gesetzgebung, Risikomanagement, Risikoberechnung und Risikonormung.

Die Fülle an Literaturquellen zum Risikomanagement wurde mehrfach zusammengefasst. Man findet Übersichten zu den Normen in Tabelle 2.6, Standardwerken in Abschnitt 2.3 und Branchen mit ausgereiften Risikomanagement in Abschnitt 2.4. Die Idee dahinter ist, dass Industrieunternehmen bestehende Methoden aus anderen Unternehmensbereichen wie dem Qualitätsmanagement oder Branchen wie der Bankenregulierung, international-financial-reporting-standard oder corporate-Ratingagenturen lernen können.

Schließlich bewährten sich die Regelwerke von COSO II und ISO 31000 als Grundstruktur für ein industrielles Risikomanagementsystem. Ein Vergleich dieser beiden recht ähnlichen Leitfäden wird in Tabelle 2.2 gezogen.

Um die gesetzlichen Mindestanforderungen übersichtlich zu klären, wurde der durch Normungen und Gesetze gültige Rechtsrahmen in Abschnitt 2.2 ermittelt und in Abschnitt 4.4 ein eigenes Reifegradmodell entwickelt. Ein Reifegrad der Stufe 1 (von 4) mit einer naiven bzw. natürlichen Herangehensweise erscheint als nicht mehr akzeptabel und muss mindestens durch eine strukturierte Herangehensweise der Stufe 2 ersetzt werden.

Die Bedeutung eines unternehmensweiten Risikomanagementansatzes und somit eines ganzheitlichen Managements aller Risiken, Chancen und Maßnahmen wird in Abschnitt 2.1 beschrieben. Ein überschlägiger Risikokalkulator in Tabelle 3.1 soll helfen die Situation des eigenen Unternehmens anhand von 9 Fragen schnell einzuschätzen.

2.1 Übersicht, Notwendigkeit und Unternehmensumfeld des Risikomanagement

Definition des Risikomanagement

Als erster Teil dieser Arbeit werden grundlegende Leitlinien bzw. Regelwerke (engl. Framework bzw. guidelines) des Risikomanagement geklärt, anhand derer sich die komplette Arbeit richtet.

Nach ISO 31000 besteht das Risikomanagement aus

> " [...] koordinierte Aktivitäten zur Lenkung und Steuerung einer Organisation bezüglich Risiken" [ISO(2009), S. 9].

Dies wird wirkungsvoll, indem die Organisation einerseits einen Rahmen für den Risikoprozess entwickelt, umsetzt und kontinuierlich verbessert. Andererseits indem der Risikoprozess überall eingebunden wird, beginnend mit der allgemeinen Führung (engl. Governance), Politik, Kultur, Strategie-, Betriebs- (engl. Operations), Planungs-, Berichterstattungs- (engl. Reporting), Compliance- bis zu den Kontrollprozessen. Diese Norm ist ein allgemeines Konzept, welches unabhängig von Branche und Risikoart, eine transparente, systematische und glaubwürdige Behandlung ermöglicht. Dabei ist das Risiko neutral zu definieren, es kann daher zu Verlusten kommen, aber auch zu positive Chancen [ISO(2009), S. 3-5].

Das COSO II Regelwerk (engl. Framework) wiederum setzt geringfügig andere Schwerpunkte, was bereits durch deren Definition greifbar wird [COSO(2009a), S. 3-5].

> "Die grundlegende Annahme des unternehmensweiten Risikomanagements ist, dass jede Organisation für spezifische Interessengruppen Werte schafft. Alle Organisationen sind hierbei Unsicherheiten ausgesetzt. Die Aufgabe der Führungskräfte ist daher zu bestimmen, wie viel Unsicherheit sie, bei dem Versuch Werte für die Interessengruppen zu schaffen, akzeptieren. Unsicherheit umfasst sowohl Risiken als auch Chancen und die Möglichkeit, Werte zu vernichten oder zu vermehren. Das unternehmensweite Risikomanagement ermöglicht daher Führungskräften wirksam mit Unsicherheit und den damit einhergehenden Risiken und Chancen umzugehen und hierbei ihre Fähigkeiten zur Wertschöpfung zu stärken. [...] Enterprise Risk Management ist ein Prozess, ausgeführt durch Überwachungs- und Leitungsorgane, Führungskräfte und Mitarbeiter einer Organisation. [sic] Angewendet bei der Strategiefestlegung und innerhalb der Gesamtorganisation, gestaltet, um die Organisation beeinflussende mögliche Ereignisse zu erkennen und um hinreichende Sicherheit bezüglich des Erreichen der Ziele der Organisation zu gewährleisten."

Ein Enterprise Risk Management nach COSO II ermöglicht [COSO(2009a), S. 3]:

- Anpassung von Risikoneigung und -strategie
- Verbesserung von risikobezogenen Entscheidungen

- Verringerung von Unvorhergesehenem und Verlusten im Unternehmen
- Bestimmung, Steuerung und Aggregation der teils mehrfach im Unternehmen vorkommenden Risiken
- Nutzen von Chancen
- Verbesserte Kapitaleinsatz
- Erreichung der gesetzten Unternehmensziele

Die beiden Definitionen zeigen ein Risikomanagement das als eigene Management-Disziplin im Unternehmen eingeführt werden soll. Andererseits bestehen in vielen Spezialgebieten bereits seit Jahrzehnten eigene risikogeführte Prozesse. In der Industrie entwickelten sich im Zuge der Industrialisierung Abteilungen für Arbeitssicherheit, funktionale Sicherheit, Qualitätssicherung [1] , Prozessmanagement [2] oder Testlabore, welche Ähnlichkeiten oder Teilaspekte des heutigen Risikomanagement aufweisen.

Allen aufgelisteten Abteilungen ist gemein, dass in einigen ihrer Aufgaben ein Risikoprozess steckt, der identifiziert, analysiert, bewertet und steuert. Das Risikomanagement als Managementdisziplin, führt nun einen vereinheitlichten Prozess unternehmensweit durch und bereitet durch Aggregation eine Filterung der Toprisiken für die Unternehmensführung vor. Denn Risiken sind wie folgendes Zitat zeigt überall.

> " To many analysts, politicians, and academics it is the management of environmental and nuclear risks, those technology-generated macro-risks that appear to threaten our existence. To bankers and financial officers it is the sophisticated use of such techniques as currency hedging and interest-rate swaps. To insurance buyers or sellers it is coordination of insurable risks and the reduction of insurance costs. To hospital administrators it may mean quality assurance. To safety professionals it is reducing accidents and injuries. In summary, risk management is a discipline for living with the possibility that future events may cause adverse effects. The general essence of risk management is about ensuring resilience to future events [McNeil et al.(2015)McNeil, Frey, and Embrechts, S. 7]."

Weitere Beispiele in denen Risikothemen in bestehenden Abteilungen und Regelungen zu finden sind, zeigt Tabelle 2.6. Details, Einschränkungen und Umsetzungsvorschläge zu beiden Risikomanagement-Leitlinien sind in Abschnitt 2.2 und Kapitel 3 beschrieben.

[1] Der Name Qualitätssicherung wurde fast vollständig durch Qualitätsmanagement ersetzt, diese wird durch die ISO 9000 und ISO 9001 genormt. Bei der Überarbeitung DIS DIN ISO 9001:2014 wird im Kp.0.5 und 6.1 erstmalig im Qualitätsmanagement ein systematischer Umgang mit Risiken und Chancen gefordert, also ein Risikomanagement.

[2] Bei allen drei gängigen Projektmanagement Standards findet sich der Risikoprozess in den Prozessen wieder, beim PMBOK Guide vgl. [PMI(2014), Kp.11], pm baseline vgl. [IPMA et al.(2006), Kp.4.1.04 und Kp.4.3.09] und DIN 69901-2 [3] .

Auslöser und Bedarf

Die Ziele eines unternehmensweiten Risikomanagements sind es, die unmittelbar vorhandenen Risiken im Unternehmen und Umwelt bewusst zu machen, sie auf ein akzeptables Maß einzugrenzen und bei jedem Risiko zu entscheiden, ob es den zu erwartenden Nutzen rechtfertigt. Es ist kein Ziel, sämtlichen Risiken aus dem Weg zu gehen, denn ein verbleibendes Restrisiko kann in keinem Unternehmen völlig eliminiert werden.

Unternehmen sind gut beraten, ihren Zugang zum Risikomanagement nach der Natur ihrer ausgesetzten Gefahren individuell auszurichten. Viel zu oft wird das Risikomanagement immer noch als Compliance Thema pauschal per Firmenregelungen und Mitarbeiteranweisungen abgehandelt. Natürlich sind Firmenregelungen per se nicht schlecht, jedoch wird regelbasiertes Risikomanagement weder die Wahrscheinlichkeit noch Bedeutung von Katastrophen reduzieren. Es bedarf einem pro-aktiven, expost, prozessintegrierten, gelebten und risikoreduzierenden Ansatz [Kaplan and Mikes(06.2012), vgl. S.5]

Abschreckende Beispiele für mangelhaftes Risikomanagement sind die hier aufgelisteten Riesenskandale oder -verluste [Denk(2008), vgl. S.5] und [Racz(2011), S.16-17]:

- Der US-amerikanischer Energieanbieter Enron bilanzierte jahrelang erfundene Fake-Profite und musste 2001 Konkurs anmelden. Darauf hin war das Vertrauen in deren Wirtschaftsprüfer Arthur Anderson so beschädigt, dass diese sich auflösten, immerhin einer der damals größten Wirtschaftsprüfer.
- WorldCom, bilanzierte 2003 vorsätzlich überbewertete Assets um deren Jahresergebnis zu beschönigen, nach der Aufdeckung dieses Fraud Falles musste Konkurs gemeldet werden. Aufgrund Enron und WorldCom wurde der Sarbanes-Oxley-Act in den USA in Kraft gesetzt und damit wiederum der COSO II.
- Die weltweiten Schmiergeld-Zahlungen von Siemens, welche während der Korruptionsaffäre 2006 bekannt wurden, erhöhte vor allem in Europa das Interesse an Compliance und guter Unternehmensführung (engl. Good Governance).
- Lehman Brothers, brachte mit ihrem Konkurs das internationale Finanzsystem ins Wanken und löste damit die weltweite Wirtschaftskrise 2008 aus
- Mangelndes Risikomanagement verursachte auch die nukleare Katastrophe von Fukushima, indem die Notstromaggregate nicht vor Jahrhundert-Flutwellen geschützt wurden..
- Massive Verzögerungen der technischen Prestigeprojekte in den 20XX Jahren. Ob Beispiele in der Luftfahrt beim A380, A350, B787, Eurofighter, F-35 oder A400 oder dem Kernkraftwerk Olkiluoto von Siemens und Areva, alle weisen massive terminliche und finanzielle Überschreitungen auf!

Diese Ereignisse führten in den letzten Jahrzehnten zu einer verstärkten gesetzlichen Regelung im Risikomanagement, wie im Abschnitt 2.2 geschildert. Diese Dynamik und einige Methoden sind nicht zuletzt durch das Basel Committee of Banking Supervision vorangetrieben worden und werden daher auch in Abschnitt 2.4 genauer geschildert . Auf die

Versicherungswirtschaft wird hier weniger eingegangen, da sie trotz Solvency Richtlinien weniger internationale Bestimmungen hat und generell weniger Beachtung findet [McNeil et al.(2015)McNeil, Frey, and Embrechts, vgl. S. 16, 30-34].

Durch die o.g. Praxisbeispiele wird die Notwendigkeit des Risikomanagement begründet, als weitere Gründe soll der Wettbewerbsvorteil durch ein unternehmensweit integriertes Risikomanagement hervorgehoben werden.

Turbulenzen sind seit jeher die primären Treiber des Risikomanagements. Die Unternehmensführung muss die Frage klären, welchen höheren Gewalten (force majeure), technischen-, rechtlichen-, oder finanziellen Problemen das eigene Unternehmen ausgesetzt ist. Zahlreiche Risiken werden als Denkanstöße in der Literatur genannt, siehe Abbildung 2.1 [Denk(2008), S. 39-41]. Durch passende Maßnahmen im Risikomanagement müssen diese dann reduziert, abgeschafft, versichert, veräußert oder bewusst übernommen werden, dazu mehr im Abschnitt 3.5.

Die steigende Komplexität und Dynamik der sozioökonomischen modernen Wirtschaft ergeben für die Bewertung im Risikomanagement meist schlecht strukturierte Problemstellungen, abhängige Risiken und schlechte Informationslage. Abhängige Risiken sind jene bei denen mehrere Quellen oder bei mehreren Risiken Kaskaden entstehen. Eine schlechte Informationslage ermöglicht meist nur schwache und unmittelbare Signale nach [Ansoff(1975b)]. Durch diese Komplexität und Dynamik soll man sich bewusst machen, dass die Analysen meist nicht präzise oder relevant sein können, aber künftig einzig durch systematisches und integriertes Risikomanagement die Risikosituation verbessert werden kann. Denn unternehmerische Intuition oder gesunder Menschenverstand stoßen heutzutage an ihre Grenzen [Romeike and Hager(2013), Kp. 2.2 und 2.3].

Es bedarf:

- nötiges Spezialwissen, wie es Dienstleister von z.B. Thomson Reuters Datastream, Bloomberg Business, The Economist Intelligence Unit Risk Snapshot oder Allianz Risk Monitor zur Verfügung stellen (siehe Kapitel 5),
- Informationssysteme die sowohl interne Kommunikation als auch wissenschaftliche Behandlung ermöglichen, siehe Kapitel 5 und Kapitel 6) und
- eine Verknüpfung des Risikomanagements mit den Prozessen,Unternehmenssteuerung, Kontrolle, Berichten und Zielen (siehe Abschnitt 4.8).

Kurz es braucht ein strukturiertes Risikomanagement. In Unternehmen herrscht jedoch weiterhin die Vernachlässigung von Wahrscheinlichkeitstheorien vor, man schaut primär auf die Renditeerwartung, ohne die damit verbunden Risiken entsprechend zu beurteilen [Romeike and Hager(2013), S. VI].

Nach den gültigen Gesetzen, siehe nächstes Abschnitt 2.2 , besteht weitestgehend noch keine vollständige Verpflichtung eines strukturierten Risikomanagements, auch wenn die Tendenzen eindeutig eine solche Entwicklung zeigen. Das bestätigt auch ein Blick in den geschichtlichen Werdegang des Risikomanagements im Abschnitt 2.5.

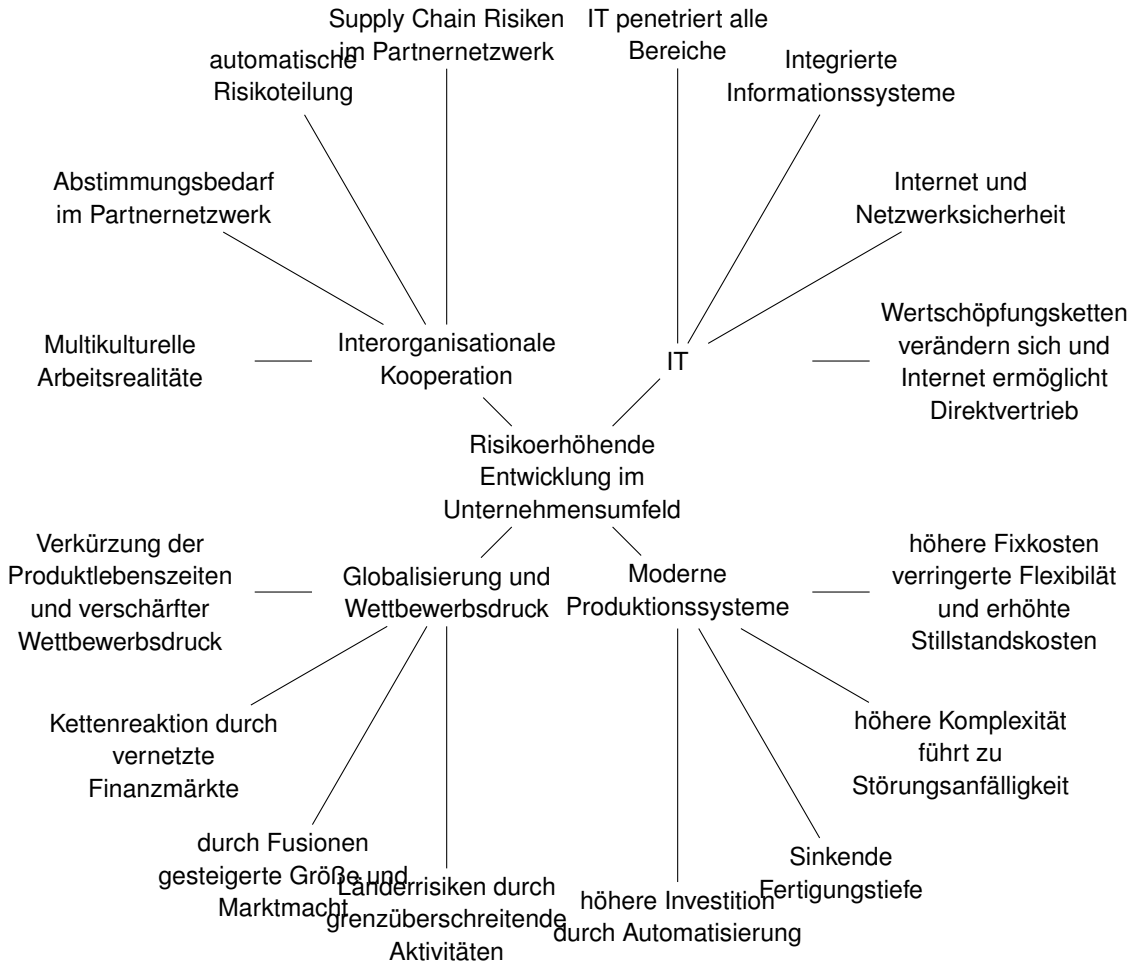


Abbildung 2.1: Risikoerhöhende Entwicklung im Unternehmensumfeld [Denk(2008), vgl. S. 39ff]

2.2 Rechtliche und normative Rahmenbedingung in Österreich

Trotz Ähnlichkeiten muss ein wesentlicher Unterschied zwischen Gesetzen, Normen und Richtlinien festgehalten werden.

- Gesetze sind vom Gesetzgeber herausgebracht und damit nicht diskutierbar und vollständig einzuhalten.
- Normen sind Regeln und Leitlinien die von staatlich anerkannten Organisationen und deren Gremien ausgearbeitet wurden. Sie lassen sich in nationale oder internationale Normungsinstitute unterteilen und sind je nach relevantem Gesetzgeberland und Branche einzuhalten. Denn Normen spiegeln den Stand der Technik wieder und dieser ist bei nicht fahrlässigen Handeln einzuhalten.

- Richtlinien können von Verbänden, Vereinen, Kammern oder Firmen herausgegeben werden und sind unverbindliche Empfehlungen aus der Praxis.

Eine Übersicht über die rechtlich relevanten Gesetze und Normungen in Österreich geben die Tabelle 2.1 und Tabelle 2.6. Die zeitliche Entwicklung der relevanten Risikomanagement Regulierungen wird durch Aneinanderreihung des Ersterscheinungsjahres dargestellt, es ist stets zu kontrollieren ob bereits aktuellere Versionen gültig sind, siehe Abschnitt 2.2 und Abschnitt 2.2 .

Gesetzliche Vorgaben

Die gesetzlichen Bestimmungen beinhalten eine ähnliche Themenfülle wie das Risikomanagement selbst. Das beiliegende Kapitel dient als Überblick der wesentlichsten Rechtsvorschriften für Unternehmen und kann als Lex generalis angesehen werden. Unternehmenspezifischere Gesetze in Abhängigkeit der Branche und Tätigkeit (Lex specialis) verdrängen etwaige hier aufgelistete allgemeinere Rechtstexte (lex generalis). So gelten zum Beispiel in der Finanzindustrie für Banken das nationale Bankwesengesetz (BWG) mit den eingearbeiteten internationalen Basel I, II, III Bestimmungen, siehe Abschnitt 2.4 [4].

Gleiches gilt für einschlägige industrielle Themengebiete die strengere Vorkehrungen bei spezialisierten Risiken beinhalten können, so z.B. Wettbewerbsrecht, Datenschutz, Arbeitsschutz, Lebensmittelsicherheit, Baurecht, etc. Die betreffenden Gesetze muss jedes Unternehmen individuell im Überblick behalten, wobei einzelne Themen selbstverständlich gesondert vom Risikomanagement und von eigenen Verantwortungsbereichen abgehandelt werden können.

Die gesetzlichen Pflichten im Risikomanagement gehen in Österreich vor allem auf die Überwachung und Berichterstattung ein.

- Überwachung lässt sich indirekt aus der fundamentalen Sorgfaltspflicht einer ordentlichen Geschäftsführung ableiten vgl. [RMA(2011), S.6].

- Berichterstattung bezieht sich auf die nach Unternehmensrechts-Änderungsgesetz (URÄG) 2008 neugeregelten Publizitätspflichten des Jahresabschlusses welche je nach Gesellschaftsform Risiken indirekt mit einbeziehen. Die URÄG 2008 setzt dabei die europäische Abschlussprüfungsrichtlinie 2006/43/EG und die Änderungsrichtlinie 2006/46/EG in nationales Recht um, vgl. [Oelkers and Bitzyk(2009), S.6]

Die Regelungen in Österreich sind damit noch nicht so streng wie in anderen Ländern. Es wird lediglich die Einführung eines internen Kontrollsystems explizit gefordert. Mit einer künftigen Verschärfung muss somit gerechnet werden. Der deutsche Gesetzgeber ist bei der Forderung nach einem Risikomanagement bereits expliziter, z.B. beim deutschen KONTRAG oder AktG §91.(2) welches bei der Organisation ein Überwachungssystem fordert, das gefährdende Entwicklungen früh erkennt. Dort ist der Vorstand verantwortlich ein Risikomanagementsystem einzuführen. Auch das US-Wertpapiergesetz ist seit 30. Juli 2002 durch

[4] vgl. https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20004983 (03.08.2014).

den Sarbanes Oxley Act Sections 302 und 404 mit mehreren Anforderungen betroffen. Aufgelistet sind unter anderem die Rotation von unabhängigen Wirtschaftsprüfern, strenge Finanzberichterstattung, Corporate Governance und das Risikomanagement als Komponente des geforderten internen Kontrollsystems [Denk(2008), S.50-53].

Folgende in Tabelle 2.1 ersichtliche österreichische Gesetze erfordern ein adäquates Risikomanagementsystem im Unternehmen:

Prüfungsausschuss für mittelständische Unternehmen

Durch das URÄG 2008 haben börsennotierte Unternehmen oder nicht gelistete Unternehmen mit einer Bilanzsumme über 96,25 Mio Euro oder Umsatzerlöse über 192,5 Mio Euro, einen Prüfungsausschuss im Aufsichtsrat einzurichten. Wie in Abschnitt 2.2 erwähnt, gehört die Überwachung der Wirksamkeit des Risikomanagementsystems mit unten aufgelisteten Fragestellungen zu deren Aufgaben, ebenso wie die des Internen Kontrollsystems (IKS) und eines allfälligen internen Revisionssystems. Letztere beide Abteilungen werden in dieser Arbeit nicht im Detail aufgeschlüsselt, sind aber in der Fußnote gut einsehbar. [6] .

- Ist ein Risikomanagementsystem eingerichtet?
- Welche Prozesse bestehen, um wesentliche Unternehmensrisiken zu identifizieren und auf ein bewusst festgesetztes Ausmaß zu vermindern?
- Sind diese Prozesse wirksam? Wird ihre Wirksamkeit regelmäßig beurteilt?
- Sind die Risiken mit Geldeinheiten bewertet und wurde eine Eintrittswahrscheinlichkeit ermittelt?
- Wie erfolgt die Dokumentation des Systems? Gibt es ein Risikohandbuch?
- Ist sicher gestellt, dass die Geschäftsführung alle relevanten Hinweise/Warnungen erhält?
- Wie wird über das System im Aufsichtsrat berichtet?
- Wie wird der Aufsichtsrat über riskante Geschäfte informiert? Gibt es einen Katalog zustimmungspflichtiger Geschäfte, nach dem besonders riskante Geschäfte der Zustimmung des Aufsichtsrats bedürfen?

Auch COSO hat speziell für kleine Unternehmen einen eigenen Leitfaden zur internen Kontrolle herausgebracht [COSO(2006), Volume I].

[6] vgl. http://wien.arbeiterkammer.at/service/betriebsrat/ifamaufsichtsrat/ifamneu/Risikomanagement_und_internes_Kontrollsystem.html (03.08.2014).

Risikorelevante Rechtspassagen	Beschreibung der betroffenen Bereiche, Tätigkeiten und Verantwortlichen
§347 UGB, §25 GmbHG und §70 AktG	Für unternehmensbezogene Geschäfte gilt die Sorgfaltspflicht seitens der Unternehmensleitung (§347 UGB, §25 Abs. 1 GmbHG und §70 AktG Abs. 1).
§22 Abs. 1 GmbHG und §82 AktG	Für Kapitalgesellschaften bedeutet das insbesondere die Schaffung eines internen Kontrollsystems neben dem ordnungsgemäßen Rechnungswesen.
Unternehmensrechtänderungsgesetz 2008 (URÄG 2008)	Mehrere österreichische Bundesgesetze fordern u.a. Compliance-Systeme, internationale Rechnungslegung, Jahresabschlüsse, Corporate Governance, Kontrollsysteme und insbesondere auch Risikomanagement. Diese Gesetze sind im betrieblichen und öffentlichen Interesse. Verweis u.a. auf das Unternehmensgesetzbuch, das Aktiengesetz 1965, das GmbH-Gesetz, das Bankwesengesetz und das Versicherungsaufsichtsgesetz. [5]
§92 Abs. 4a Z 2 AktG und §30g Abs. 4a Z 2 GmbHG	Seit URÄG 2008 sind die Aufsichtsorgane von Kapitalgesellschaften für die Überwachung der Wirksamkeit des Risikomanagementsystems verantwortlich. Wenn eine interne Revision existiert, ist diese miteinzuschließen.
§243 UGB und §267 UGB (Absatz 3 lit a und b)	Der Lagebericht oder Konzernlagebericht hat die Geschäftsverläufe und Lage des Unternehmens möglichst getreu zu beschreiben. Dies schließt die Risikomanagementziele und -methoden, Absicherungsgeschäfte und bestehende Preisänderungs-, Ausfall-, Liquiditäts- und Cashflow-Risiken mit ein.
Verbandsverantwortlichkeitsgesetz (VbVG)	Bei strafbaren Handlungen einzelner Entscheidungsträger und Mitarbeiter liegt bei mangelnder Organisationsstruktur ein Organisationsverschulden vor und somit kann das Unternehmen strafrechtlich belegt werden. Grundsätzlich gilt auch in einer Unternehmensorganisation der Vertrauensgrundsatz. In hierarchischen Organisationen gilt der Vertrauensgrundsatz nur, wenn eine sorgfältige Personalauswahl erfolgt, angemessene Kontrollmechanismen eingerichtet sind und ganz allgemein eine adäquate Ablauforganisation eingerichtet ist. Für gefährliche oder “strafgefährdete” Bereiche ist durch organisatorische Maßnahmen sicherzustellen, dass die Verbandspflichten eingehalten werden.
Austrian Code of Corporate Governance	Dieser repräsentativ zusammengesetzte Arbeitskreis aus UnternehmensvertreterInnen ist nicht verbindlich und beruht auf freiwilligen Selbstregulierungsmaßnahmen. Zumindest für Aktiengesellschaften kann er indirekt als verbindlich angesehen werden, da für eine Listung an der Wiener Börse dessen Einhaltung verpflichtend ist. Die Paragraphen 9, 18, 37, 40, 67, 69 und 80 befassen sich mit Risikomanagement und beruhen auf zwingenden Rechtsvorschriften [ÖCGK(2015), vgl. S.12-14].
IRÄG	Insolvenzrechtsänderungsgesetz 2010 befasst sich mit Instrumenten zur Früherkennung von Problemsituationen wie Insolvenz [Denk(2008), S.52].

Tabelle 2.1: Übersicht der rechtlichen Bestimmungen bezüglich Risikomanagement in Österreich [RMA(2011), S.6ff] und [Denk(2008), S.42ff]

Risiko im Corporate Governance Kodex

Dem Zeitgeist folgend fanden Risikobetrachtungen auch Einklang in den Empfehlungen guter Corporate Governance, also guter Unternehmungsführung und internationaler Rechnungslegung und ist somit auf jeder Ebene des betrieblichen Alltags relevant.

So forderte bereits 1998 das deutsche Gesetze zur Kontrolle und Transparenz im Unternehmensbereich (kurz KonTraG) ein Risikomanagement und -controlling, auch wenn diese bei der konkreten Ausgestaltung vage bleibt. International wurde das KonTraG Ausgangspunkt von Risikofrüherkennungs-, und überwachungssystemen vgl. [DGR(2008), S.3ff]. Für die Praxis bedeutsam vgl. [Diederichs(2012), S.25] waren vor allem die

- Implementierung eines Risikofrüherkennungs-, und überwachsungssystems,
- die Prüfung des ersten Punktes durch die Wirtschaftsprüfer und Berichterstattung an den Aufsichtsrat
- die Erweiterung im Lagebericht um die Risikoberichterstattung und Plausibilitätsprüfung durch den Wirtschaftsprüfer.

In Österreich behandelte der Corporate Governance Kodex erstmalig 2002 ein Risikomanagement auf Basis von Selbstregulierung und dem sogenannten Comply or Explain-Prinzip, welche bei Nicht-Einhaltung der Empfehlung eine Erklärung fordert. Besonders die folgenden Paragraphen beruhen auf zwingenden Rechtsvorschriften:

- § 9 Beschäftigung der Risikosituation im Aufsichtsrat
- § 40 Effizienz des unternehmensweiten Risikomanagementsystems
- § 69 Konzernlagebericht legt die Situation der Gesellschaft und des Risikomanagement dar

Der sogenannte “swiss code of best practice for corporate governance” wurde am 1.Juli 2002 als ebenfalls freiwillige Verhaltensregeln in der Schweiz eingeführt. Er umfasst in der aktuellen Ausgabe vom 28. August 2014 die vier Themenfelder Aktionäre, Verwaltungsrat / Geschäftsleitung, die Revision und die Offenlegung. Für deren Erfüllung sind insgesamt 29 Leitsätze nötig. Der Anhang über spezifisch schweizerische Vergütungsregeln kann ignoriert werden.

Risiko Management Normen und Leitfäden

Die in dieser Arbeit verwendeten gängigen Normenwerke sind die von COSO II Enterprise Risk Management Framework und ISO 31000 Risikomanagement - Grundsätze und Leitlinien. Vor allem die Anwenderhandbücher des COSO II Framework, der ONR 49000-Serie als Umsetzungsleitfaden der ISO 31000 und das angloamerikanische Handbuch “HB 436:2004 Riskmanagement Guidelines Companion for AS/NZS 4360” sind gute Hilfsmittel für die Industrieanwendung.

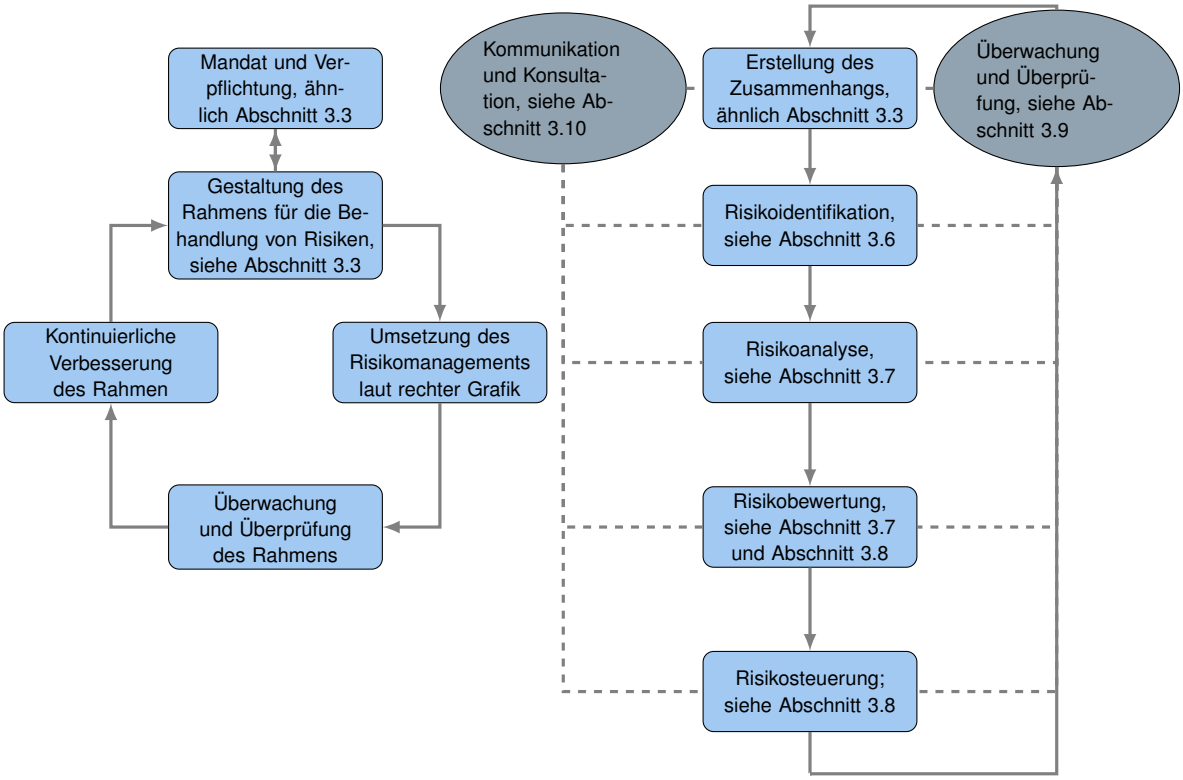


Abbildung 2.2: Risikomanagement nach ISO31000 [ISO(2009), Bild1]

Für eine praktische Anwendung bei einem mittelständischen Industrieunternehmen wurden die ISO 31000:2009 als generisches Rahmenwerk und der COSO II ERM:2004 als praktisches Umsetzungshandbuch gewählt. In Anbetracht des Alters beider Werke erscheint eine baldige Neugestaltung als wahrscheinlich, ebenfalls wird im Folgenden auf die aktuelle Kritik gegenüber beider Normen eingegangen.

Abschnitt 2.6 zeigt eine historische Übersicht über die Entwicklung der einschlägigen Normen und Leitfäden. Diese sind meist mehrteilig aufgebaut, zuerst wird eine generische Übersicht als Grundlage eingeführt und danach bilden weitere Teile Spezialthemen oder Anwenderhandbücher ab.

Übersicht der ISO31000 Risiko Management Norm

Die Abbildung 2.2 zeigt den in dieser Arbeit verwendeten Risikomanagementsystem Ansatz nach [ISO(2009), Bild 1].

Beschreibung der ISO 31000 [ISO(2009), S.16ff] wird in die zwei PDCA-Deming-Kreisläufe des Rahmens und Prozesses unterteilt. Dabei wird in einem kontinuierlichen Verbesserungsprozess laufend geplant (plan), umgesetzt (do), überprüft (control) und erneuert (act).

1. **Risikomanagementrahmen** - Die Geschäftsführung legt anhand dessen die Ziele des Risikomanagements im Einklang mit den Unternehmenszielen fest. Die Methoden, Organisationsaufbau und Ressourcen werden hier vorgeben.

2. **Risikomanagementprozess** - Im Zuge des Risikomanagementprozesses werden in allen Abteilungen Ereignisse als Risiken oder Chancen systematisch identifiziert, bewertet und bewältigt. Dafür bedarf es den üblichen Managementgrundsätzen.

3. **Kommunikation, Überwachung, Überprüfung, Verbesserung** - Parallel findet eine Überwachung seitens des zentralen Risikomanagers statt, der auch für die ständigen Verbesserungen, das Informationssystem und Reporting zuständig ist.

Die Norm weist ausdrücklich darauf hin, dass jede spezifische Branche und Anwendung einen individuellen Zusammenhang erstellen muss. Diese kann auf veränderliche Erfordernisse, Sichtweisen oder Kriterien eingehen oder Besonderheiten im Unternehmen bei Zielgruppen, Zielen, Aufbau, Prozessen, Firmenkultur, Funktionen, Projekten, Produkten, Dienstleistungen, Zeitdauer oder Vermögen beinhalten. Es ist somit auch kein vereinheitlichtes Risikomanagementsystem gewollt oder möglich [ISO(2009), S. 8].

Die Etablierung einer Mutternorm für das Risikomanagement scheint mit der ISO 31000 derzeit nicht möglich zu sein. So meldete der dafür zuständige DIN-Normenausschuss für Sicherheitstechnische Grundsätze im September 2011, dass sie für eine ersatzlose Streichung der ISO31000 sind. Jedoch wurde beim internationalen Ausschuss der ISO/TC 262 Risikomanagement eine begrenzte Überarbeitung vereinbart [7]. Die offizielle internationale Risikomanagement Normung ist demnach gespalten und die ISO 31000 steht in der Kritik.

Übersicht der COSO II ERM Risiko Management Norm

Abbildung 2.3 zeigt den Aufbau der COSO II Risikomanagement Komponenten, diese werden schrittweise als Prozess abgearbeitet. Der ursprüngliche COSO II Würfel verknüpft die Risiko-Komponenten noch mit den zwei weiteren Dimensionen, erstens den Zielen und zweitens der Organisationshierarchie. Diese beiden Dimensionen sind im Datenmodell Abschnitt 6.2 des Informationssystem berücksichtigt, in der Abbildung Abbildung 2.3 aber zwecks Übersichtlichkeit vernachlässigt.

Auch die Einführung des COSO II Frameworks führt zu keiner hundertprozentigen Sicherheit. Unsicherheiten bestehen bei der teils unlogischen Risikoaversion während der menschlichen Urteilsbildung durch sogenannte Heuristiken, dem Spannungsfeld zwischen Kosten und Nutzen oder operativen Risiken wie z.B. Betrug und wenn Führungskräfte das Risikomanagement außer Kraft setzen. Daher wird auch eine Zusammenarbeit mit dem internen Kontrollsystem empfohlen [COSO(2009a), S.7].

Kritik um die Vernunft des COSO Frameworks:

[7] http://www.din.de/de/mitwirken/normenausschuesse/nasg/iso-tc-262-beschliesst-begrenzte-ueberarbeitung-der-iso-31000-2009-und-des-iso-guides-73-2009-78322 und http://www.din.de/de/mitwirken/normenausschuesse/nasg/iso-31000-2009-wird-endgueltig-nicht-ins-deutsche-normenwerk-uebernommen-75964

Internes Umfeld - Risikomanagementphilosophie-, bereitschaft-, kultur, Geschäftsleitung, Organisationsstruktur, Aufgabenverteilung, Personalstandards
Zielfestlegung - Strategische- und daraus abgeleitete Ziele, Risikobereitschaft und -toleranz
Ereignisidentifikation - Risiken oder Chancen, Einflussfaktoren, Identifikationstechniken, Korrelationen, Kategorisierung
Risikobewertung - Inhärente und Restrisiken, Ermittlung von Eintrittswahrscheinlichkeit und Auswirkung, Datenquellen, Bewertungsmethoden, Zusammenhänge zwischen Risiken bzw. Chancen
Risikosteuerung - Bewertungen und Auswahl mittels Maßnahmenkatalog und Risiko-Portfolio als Gegenüberstellung von Risikobereitschaft und Restrisikoprofil
Kontrollaktivität - Integration mit Risikosteuerung, Typen von Kontrollmaßnahmen, Präventiv-, und aufdeckende Maßnahmen, Regelungen, Verfahren, Kontrolle der Informationssysteme, Organisationseinbindung
Information und Kommunikation - interne und externe Quellen mit aktuellen und vergangenen Daten, relevantes aus Rohdaten extrahieren, präzise Kommunikationswege, klarer tone-of-the-top, informierte Mitarbeiter, Whistleblower-System, Behördenbetreuung
Überwachung - Laufende Überwachungsmaßnahmen, gesonderte Audits, Mängelberichterstattung und deren Reparaturüberwachung

Abbildung 2.3: Beschreibung der Kategorien des COSO II Risikomanagement [COSO(2009a), Abb. 1.1] und Verknüpfung mit den ISO 31000 Elementen

- Die Norm ist sehr generisch und allgemein gehalten. Daher braucht man für eine reale Umsetzung der kritischen Komponenten spezifischere Methoden aus der Fachliteratur, besonders fällt dies bei der Risikoaggregation-, und quantifizierung auf. Weiters wird nicht auf eine IT-gerechte Umsetzung des Risikomanagement eingegangen.

- COSO I wurde in den 1990er Jahren verfasst und entspricht damaligen Standards. Seither wurde unter anderem durch die Basel Regelungen eine wissenschaftlichere Risikobewertung entwickelt, z.B. bei der Quantifizierung von Risiken durch historische Sammlungen von Verlustdaten. Diese modernen Ansätze sind in Coso II nicht enthalten [OpRisk-Advisory and Towers-Perrin(2010), S.27].

- Die starke Orientierung COSO II an die Bedürfnisse der Wirtschaftsprüfer bzw. der Revision. Dies ist mit der Herkunft bzw. Ableitung des COSO II aus dem COSO I

begründet. Denn auch der COSO II legt einen klaren Fokus auf die Umsetzung eines risikoorientierten internen Kontrollsystems [Denk(2008), S.55].

- Robert S. Kaplan (unter anderem Erfinder der Business Score Card) stellt fest, das Risikomanagement am besten mit Dialog und nicht Regeln geführt wird. Weiters wird es in seinen Augen zu oft wie ein Compliance Thema behandelt und die menschlichen Schwächen unterschätzt, bei Einschätzung (Heuristik) und sträubender Behandlung von Risiken. Das Risikomanagement muss als unabhängige Abteilung Spezialwissen aufbauen und gegenüber den Einschätzungen der Risikoeigner eine kritische Eigenbewertung wahren. Die gesetzlichen Regeln übersehen, dass eine Risikomanagement Größe nicht allen Unternehmen passen kann. [Kaplan and Mikes(06.2012), S.1ff]

- Der COSO II Framework ist durch seine allgemeine Formulierung und uneingeschränkt-unternehmensweite Anwendung sehr ressourcenintensiv und auditbasierend. Gravierend ist vor allem die Gefahr, dass durch diese ausführliche Herangehensweise bereits bei der Identifikation unübersichtlich viele Risiken erfasst werden, welche noch dazu redundant (nicht unabhängig) zu einander sind. Die wenigen, wichtigen Toprisiken können von den vielen trivialen Risiken überdeckt werden.

- Einer bottom-up Risikobeurteilung durch die Risikoeigner selbst wird nach Auffassung von [OpRisk-Advisory and Towers-Perrin(2010), Exhibit 1.1] abgeraten. Diese seien meist subjektiv und gefesselt von trivialen Alltagsrisiken! Es wird eine top-down Analyse der Toprisiken innerhalb von scharf definierten und nicht zusammenhängenden Risikoklassen empfohlen. Diese wenigen Toprisiken sollen dann im Detail und mittels historischer Daten in Form von Verteilungsfunktionen berechnet werden. Weiters soll auf jeden Fall die Frequenz statt der Wahrscheinlichkeit verwendet werden, da diese auch aggregierbar sind und mittels Szenarien wie Durchschnitt oder Worst-case quantifiziert werden können.

- Die operationellen Risiken (kurz Oprisk), zu denen im Mikrobereich menschliches Versagen aber auch Betrug zählen, werden zwar durch COSO oder Basel in der Kontrolle behandelt und sind abschätzbar. Doch die unternehmensbedrohlichsten Oprisk auf der Makroebene werden bei COSO systematisch unterschätzt. Dies sind die schwer abschätzbaren abnormalen Oprisks, wie force majeure oder risikofördernde Kultur. Ebenfalls unterschätzt werden auch jene großen Oprisk durch Entscheidungen der Unternehmensführung, wie Automatisierung, E-Commerce, Systemintegration durch Mergers and Acquisitions, Outsourcing oder komplizierte Finanzierungsmethoden. Zumindest bei Banken sind diese großen Oprisk zwar nur 1% der Events lösen aber 60-70 % des Gesamtschadens aus [OpRisk-Advisory and Towers-Perrin(2010), Kp.5].

- Die von COSO vorgeschlagene Ermittlung des Risikos mittels Multiplikation von Häufigkeit mal Auswirkung erscheint in der Versicherungsmathematik bzw. dem Risikomanagement als falsch. In der Versicherungsmathematik sind die Toprisiken jene mit geringster Frequenz und höchster Auswirkung, von Nassim Taleb so genannte

COSO Komponenten	ISO31000 Elementen
Internes Umfeld	ISO 4.2 bis 4.6 und 5.3
Zielfestlegung	ISO 5.3, 4.2 und 4.3.2
Ereignisidentifikation	ISO 5.4.2
Risikobewertung	ISO 5.4.3 und 5.4.4
Risikosteuerung	ISO 5.5
Kontrollaktivität	ISO 4.5, 5.2 und 5.6
Information und Kommunikation	ISO 4.3.6, 4.3.7 und 5.7
Überwachung	ISO 4.5, 4.6 und 5.6

Tabelle 2.2: Übertragungstabelle - Ähnlichkeiten zwischen COSO II Komponenten und ISO31000 Elementen [ISO(2009), S.16ff] [COSO(2009a), S.27ff]

schwarze Schwäne. Bei COSO sind die kritischsten Risiken (=Toprisiken) somit jene mit höchster Häufigkeit und höchster Auswirkung. Das ist unlogisch, denn Risiken mit hoher Auswirkung und gleichzeitig hoher Häufigkeit gibt es gar nicht, so Ali Samad-Khan [OpRisk-Advisory and Towers-Perrin(2010), Kp. 3.2 und 4.].

Tabelle 2.2 vergleicht die einzelnen COSO II Komponenten mit jenen äquivalenten der ISO31000 Elementen. Dies ermöglicht ähnliche Aufgaben beider Normen zuzuordnen und damit auch sicher zu stellen, dass das Risikomanagement mit beiden Normen konform ist.

Das in dieser Arbeit aufgebaute unternehmensweite Risikomanagementsystem ist an diesen beiden Normen angelehnt. Es gibt noch andere Risikomanagementsysteme, eine Variante die von einem Beratungsunternehmen erstellt wurde, wird in Abschnitt 4.9 gezeigt.

2.3 Weitere Standardwerke im Risikomanagement

Sowohl in der deutschen als auch englischsprachigen Fachliteratur kursieren eine Fülle an ähnlichen Methoden und Begriffen im Risikomanagement, es hat sich bisher kein einheitlicher Standard entwickelt [Diederichs(2012), S. 8 -10].

Diese Arbeit erhebt den Anspruch, eine praxisnahe Aufarbeitung und Umsetzung eines Risikomanagementsystemes zu sein. Im Allgemeinen und im Speziellen bei der Umsetzung innerhalb eines Informationssystems. Trotz der Fülle an Themen und veröffentlichten Werken sind die Folgenden besonders zu empfehlen:

1. Beim Aufbau eines unternehmensweiten Risikomanagementsystems, befassen sich im deutschsprachigen Raum seit Jahrzehnten Brühwiler, Gleißner, Romeike [8] und Embrechts [9] mit praktischen und ähnlichen Ansätzen. Die Bücher [Denk(2008)], [Gleissner(2011)], [Romeike and Hager(2013)], [Brühwiler and Romeike(2010)] und [McNeil

[8] Deren gemeinsames Netzwerk und Wissenspool seit 1998 besteht, siehe `http://www.risknet.de`

[9] Auf seiner Homepage befinden sich eine Fülle an beantworteten Forschungsfragen, Quellen entlehnter Ideen aus allen Wissenschaftsfeldern und Denkanstöße bezüglich Risiko `https://people.math.ethz.ch/~embrecht/`. Weitere Dienste werden als Beratung angeboten, siehe `www.riskcenter.ethz.ch`.

et al.(2015)McNeil, Frey, and Embrechts] zeichnen sich durch gute Lesbarkeit und vernünftige Lösungsvorschläge aus. Im englischen Sprachraum sind dies [Kaplan and Mikes(06.2012)], [Damodaran(2008)] und [Marco and Lister(1987)].

2. Auch Normungsinstitute oder Standardwerke von normungsähnlichen Verbänden sind zahlreich vorhanden. Sie bieten einen wertvollen Schatz an Praxiserfahrungen und Anwendungsbeispielen, siehe [COSO(2009a)], [ONR(2014b)], [ÖCGK(2015)] und [RMA(2011)]. Auch diverse Berufsgruppenverbände geben Positionspapiere zum Risikomanagement heraus, vor allem die angloamerikanischen “Institute of Chartered Accountants”, “Institute of Certified Public Accountantsöder İnstitute of actuaries” (dt. Aktuar) sind zu beachten.

3. Die großen Strategieberatungsunternehmen behandeln seit Jahren das Risikomanagement. Interessante Best-Practise Beispiele sind McKinseys “working paper on Risk” [10], “Accenture - Global Risk Management Study” [11] und einige PWC Studien über den deutschen Mittelstand [12].

4. Quantifizierung von Einzelrisiken und deren Aggregation zu unternehmensweiten Toprisiken werden in [DGR(2008)], [OpRisk-Advisory and Towers-Perrin(2010)], [Basel(2009)] oder [Basel(2010a)] [13] behandelt.

5. Risikodaten sind auf Ebene der Makroökonomie relativ frei zugänglich, vor allem durch die Statistik Austria, OECD oder Eurostat [14].

6. Detaillierte aufs eigene Unternehmen übertragbare, makroökonomische Risikodaten sind dabei meistens schwerer zugänglich. Weltweite Dienstleister können teilweise Abhilfe schaffen, z.B. Thomson Reuters Datastream, Bloomberg Terminal, The Economist Intelligence Unit, Allianz Risk Monitor oder Business Intelligence Anbieter SAS Knowledge Base [15].

7. Ebenso gibt es eine Fülle an diversen Dienstleistern für spezielle oder nationale Risikokategorien, z.B. die großen 3 angloamerikanischen Ratingagenturen Standard & Poor, Moody und Fitch Rating oder der österreichische KSV1870 bei Kreditratings von Unternehmen [16].

---

[10] http://www.mckinsey.com/client_service/risk/latest_thinking/working_papers_on_risk

[11] https://www.accenture.com/dk-en/global-risk-management-research-2015.aspx

[12] http://www.pwc.de/de/risk.html

[13] http://www.bis.org

[14] www.statistik.at, https://data.oecd.org und ec.europa.eu/eurostat/

[15] http://thomsonreuters.com/en/products-services/financial/investment-management/datastream-professional.html, http://www.bloomberg.com/professional/hardware/, http://www.eiu.com, https://www.allianzglobalinvestors.de/ oder http://support.sas.com/resources/

[16] https://www.ksv.at

8. Für Informationssysteme als Disziplin der Wirtschaftsinformatik, sind für alle nicht einschlägig IT-bewanderten Praktiker die Werke von [Krcmar(2015)] und [Abts and Mülder(2013)] zu empfehlen, sie behandeln das minimal nötige. Spezialwissen wie die benutzerfreundliche Aufarbeitung in Form von Datenbanken oder Benutzeroberflächen (engl. Dashboards und als Überbegriff "Human user interface") benötigen einschlägige Expertise. Anhaltspunkte können dafür z.B: "Gartner magic quadrants" [17] geben.

9. Auf Risikomanagement spezialisierte Informationssysteme oder Teilmodule findet man bereits bei fast allen ERM-Anbietern (Enterprise Ressource Management), siehe dafür Abbildung 5.5.

10. Ein Blick auf hochspezialisierte Anbieter der Finanzindustrie lohnt sich bei ambitionierten Unternehmen, denn dort findet sich möglicherweise die Technologie von Morgen. Beispiele hierfür sind die hauseigene Plattform Aladdin des 3.700 MRD $ Assetmanager (2011) BlackRock. Bei einem Interview 2004 erklärte BlackRock Vice Chairman Rob Kapito, dass Aladdin selbst aufgebaut wurde, da es damals nur glorifizierte Tabellenprogramme gab, aber keine Informationssysteme, sein Ratschlag für ein Informationssystem ist "Eine Datenbank, ein System und ein Prozess. Dann schauen alle im Unternehmen auf das Gleiche" [18] . Auch die geheimdienstnahe Palantir, bietet mehrere Datenanalyse-und Planungssysteme [19] .

Unterschiede in der englischen und deutschen Wissenschaftskultur

Beim Heranziehen der angelsächsischen Normung des Risikomanagements und Literatur sei auf eine unterschiedliche Wissenschaftskultur-, und tradition hingewiesen. Da das Risikomanagement wesentliche Impulse aus diesen Ländern erhält, kommt man kaum umhin sich auch mit englischsprachiger Fachliteratur zu beschäftigen. Nach dem Linguisten Winfried Thielmann verbergen sich in englischen Publikationen hinter der meist gut leserlichen populärwissenschaftlichen Sprache und deren vermeintliche Leichtigkeit, für deutsche Leser erhebliche Missverständnisse. Im Vergleich zur deutschsprachigen Literatur unterscheiden sich bei angloamerikanischen Werken die Argumentationstechnik oder englische Traditionen im linearen Aufbau der Arbeiten. Gegenseitiges Unverständnis dem deutschen bzw. englischen Formalismus gegenüber und nicht zu unterschätzende sogenannte false-friends Vokabel sind weitere Fehlerquellen, siehe Abschnitt 3.2 . [20]

---

[17] http://www.gartner.com/technology/research/methodologies/magicQuadrants.jsp

[18] http://www2.blackrock.com/us/brs, http://www.economist.com/news/briefing/21591164-getting-15-trillion-assets-single-risk-management-system-huge-achievement (6.12.2013) und http://www.wallstreetandtech.com/asset-management/how-blackrock-stays-solid/17200108 (16.9.2015)

[19] http://www.economist.com/node/21554743(16.9.2015), http://www.palantirsolutions.com

[20] vgl. http://www.sueddeutsche.de/karriere/wissenschaftliche-aufsaetze-ein-bisschen-englisch-reicht-nicht-1.986666-2(03.08.2014).

Abgrenzung zur Populärwissenschaft

Warum lohnt sich deren Betrachtung? Das Risikomanagement als interdisziplinäre Disziplin zwischen Betriebswirtschaft, Management, Psychologie und Finanzmathematik umfasst das gesamte Unternehmen mit allen Mitarbeitern und Prozessen.

Für den angewandten Aufbau eines klassischen und gesetzkonformen Risikomanagements sind die populärwissenschaftlichen Werke nicht notwendig. Die dabei behandelten Themen können aber als Anregung dienen.

- In der Heuristik Forschung wird das menschliches Verhalten untersucht. Aus psychologischen Versuchen werden so Rückschlüsse auf die Risikokultur und deren handelnden Risikoverantwortlichen zugelassen. Zu empfehlen sind [Gigerenzer and Kober(2013)] und [Kahneman(2011)]. Kahneman erhielt für seine Forschung über die Verhaltensökonomik (engl. behavoural economics) 2012 den Wirtschafts-Nobelpreis. Als weltklasse Verhaltensforscher zählt auch Ernst Fehr, dieser betreibt neben seiner Professur auch eine Beratungsfirma [21] Ankerheuristiken und Kognitionspsychologie sind bereits in Standardwerken des Risikomanagement zu finden [Romeike and Hager(2013), S. VI].
- Warnungen vor der ungestümen Verwendung von branchenfremden Methoden oder beim Umgang mit Risiken in Bezug auf statistisch seltene Großkatastrophen finden sich bei Nassim Taleb, [Taleb(2008)] und [Taleb(2012)]. Diese nach Taleb sogenannten schwarzen Schwäne gehören in jedem Unternehmen ausgiebig beurteilt und behandelt. Zuvor fand man sie meist nur als force majeure Klauseln im Vertragswerk, um die höhere Gewalt im Tiefbau oder Projektgeschäft insofern zu regeln, dass man sie als nicht kontrollierbar auf die Auftraggeber abwälzt.

2.4 Risikomanagement in der Finanzregulierung von BASEL, IFRS bis zu Rating Agenturen

Eine Beschäftigung mit risikorelevanten Finanzregulierung ist auch für Unternehmen die nicht zur Finanzbranche gehören sinnvoll. Die Beschäftigung mit Risiken ist eine der Finanzindustrie immanente Kerntätigkeit, somit sind die Methoden der Risikoaggregation- und Risikoquantifizierung dort auch am weitesten Fortgeschritten. Am Ende dies Unterkapitels wird auf nötige finanztechnische Grundlagen im Risikomanagement eingegangen.

Risiko im International Financial Reporting Standards (IFRS)

Auch die übernationale International Financial Reporting Standards (IFRS) behandelt Risiken, im Besonderen im Rahmen der IFRS 7 und 9 welche die Offenlegung von Risiken der wichtigsten Finanzinstrumente und ausdrücklich deren Risikomanagement fordert [Christian and Lüdenbach(2013), S.51ff]. Dabei wird die Natur, Ausmaß und Management der Kredit-,

[21] vgl. `http://www.econ.uzh.ch/en/faculty/fehr.html` und `http://www.fehradvice.com/unsere_kompetenzen`.

Liquiditäts-, und Marktrisiken gefordert. Politische, operative oder strategische Risiken werden aufgrund des Finanzschwerpunktes der IFRS nicht behandelt.

Als Finanzinstrumente können nach IAS 32 alle finanziellen Assets betrachtet werden, bei denen mittels Vertrag eine Rendite vereinbart wurde, so zum Beispiel trade receivables, trade payables, equity instruments (Aktien), bonds issued, etc. Die IFRS setzt dabei auf den fair value Ansatz mittels discounted cash flows nach IFRS 13, welche die vergangenen oder zu erwarteten Cashflows an den heute zu erwartenden Marktwert auf- oder abzinst.

Die von der IFRS geforderten Mindestanforderungen verbleiben bei einfachen qualitativen Entscheidungen und quantitativen Zusammenfassung der Datenquellen über Risikoaussetzung. So fordern die spezifischen Anforderungen bei:

- Kreditrisiken eine Analyse des maximalen exposure to risk, z.b. mittels Zeitreihen-Betrachtung der abgezinsten Zahlungsausfälle, Konkurse und Sicherheiten. Verlustmodelle (expected loss model) werden in IAS 39 behandelt.

- Liquiditätsrisiken eine Laufzeiten (Maturity) Analyse der fix und variabel verzinsten Finanzinstrumente, wie zum Beispiel Fremdkredite, unter worst-case Annahme der frühestmöglichen Fälligkeit.

- Marktrisiken eine Sensitivitätsanalyse, also die simulierten Veränderungen der wesentlichen Marktkennzahlen wie Leitzins, Währungen oder Rohstoffe im realistischen und möglichen Umfang nach IFRS 7.40 und mittels discounted cash flows nach IFRS 13.

Einzig die in IFRS 7 erwähnte quantitative Risikokonzentration, ist bei statistischer Anwendung abseits einer Expertenschätzung aufwendig und technisch anspruchsvoll.

Die IFRS ist seit der Übernahme bestimmter internationaler Rechnungslegungsstandards gemäß der Verordnung (EG) Nr. 1606/2002 europaweit geltendes Recht gleichzusetzen. Die Anpassung auf aktuelle Entwicklungen der IFRS erfolgt durch weitere Verordnungen, so zuletzt durch die Verordnung (EG) Nr. 1126/2008.

Auswirkungen von Basel I, II und III auf Industriebetriebe

Für jeden Sektor in der Finanzindustrie gelten unterschiedliche Regelungen, für Banken die Basel-, für Versicherungen die Solvency-, oder für Pensionskassen die PKG-Bestimmungen. Die Basel Bestimmungen des Banksektors werden in dieser Arbeit detailliert erklärt, da sie noch am ehesten Ähnlichkeit zur Industrie aufweisen. Das ist bei Solvency oder PKG definitiv nicht der Fall. Banken und Industrie haben beide Kundennähe und ihre Organisationsstrukturen von Finanz-, Verkauf- oder Risikomanagement haben Ähnlichkeit.

Die Bank for International Settlements (BIS) gibt in ihren Methodenvorschlägen daher auch einen Industriestandard wieder. Diese werden im Kapitel Abschnitt 2.4 wieder betrachtet werden. Die drei bisher veröffentlichten Basler Eigenkapitalakkorde (Basel I, II und III) werden von der 1939 gegründeten BIS in Zusammenarbeit mit ihren Mitgliedern, den nationalen Notenbanken, erstellt und dienen dem Organisationsziel der internationalen Finanz-

und Währungsstabilität [22] [McNeil et al.(2015)McNeil, Frey, and Embrechts, S.16-19 und Kp. 1.3]..

- Aufgrund von Zusammenbrüchen bedeutender Banken, regelte Basel I 1988 die Mindesteigenkapitalausstattung von Kreditinstituten in Abhängigkeit des Risikoprofils. Zuerst war dies nur das Kreditrisiko und ab 1996 auch das Marktpreisrisiko. Grundsätzlich muss das Eigenkapital 8% der risikogewichteten Kredite haben, vgl. [Pape(2011), S.246].

- 2006 wurden Erweiterungen als Basel II beschlossen, da bei Basel I das tatsächliche Risikoprofil aller Risikoklassen und -prozesse nicht ausreichend abgebildet war. Auch wurde zwischen den verschiedenen Finanzanlagen inhärente Risiken zu wenig differenziert. Die Erweiterungen zielten somit auf eine Erweiterung im Risiko- und Ertragsprofil und der Risikosteuerung ab. Dies wurde durch ein Grundkonzept mit drei Säulen aufgebaut, erstens aus einer Mindestkapitalanforderung, zweitens einen Überprüfungsprozess der Bankenaufsicht und drittens erweiterte Offenlegungspflichten [Pape(2011), vgl. S.247].

- Für Basel III begann die phasenweise Umsetzung 2013, mit einer regulierten Leverage ratio und Kapital-, und Liquiditätsstruktur welche mittels regelmässigen Stresstests kontrolliert werden. Weiters werden Maßnahmen für die Marktdisziplin, Transparenz, Risikomanagement und Governance gefordert. [23]

  - Die für eine Bank zu kontrollierenden Risiken sind die Adressenausfallrisiken, Marktrisiken, Liquiditätsrisiken und operationelle Risiken [MaRisk(2014), S.53].
  - Laut der deutschen Bundesanstalt für Finanzdienstleistungsaufsicht (kurz BaFin), ist der MaRisk-Umsetzungsleitfaden [MaRisk(2014)] eine konforme Umsetzung der Basel Bestimmungen und genügt somit geltenden europäischem und deutschem Recht [BaFin(2011), S.2] und [MaRisk(2014), S.14].

Basel wurde für international agierende Banken geschaffen. Die Grundannahmen sind, dass größere Banken besser mit Risikomanagement umgehen und daher Standardmethoden (standardised approach) durch selbstentwickelte, fortschrittliche Risikoanalyse ersetzen können (Advanced Measurement Approaches, kurz AMA), inklusive geringerer Kapitalbindung. Des Weiteren soll eine erweiterte und transparentere Veröffentlichung von Geschäftszahlen eine natürliche Marktdisziplin schaffen. [24]

Für normale Unternehmen wirken sich die Basel Bestimmungen bei der Kreditvergabe aus, da Banken seit Basel individuelle Ratings für jeden Kunden erstellen müssen, nach denen sich deren Kreditzinsen richten [Denk(2008), vgl. S.52]. Die somit zunehmende wirtschaftliche Bedeutung von Ratings bei den Finanzierungskosten und der Umstand, dass

[22] vgl. `http://www.bis.org/about/index.htm(05.08.2014)`.

[23] `http://www.bis.org/bcbs/basel3.htm` (05.08.2014).

[24] vgl. One Basel leads to another vom 18. Mai 2006, `http://www.economist.com/node/6908488/print?story_id=6908488` (05.08.2014).

die Bewertung des Risikomanagements ein Teil der Ratingbeurteilung ist, werden im Abschnitt 2.4 behandelt. Obwohl sie für den Banksektor entworfen wurden, sind die Baselregelungen auch für andere Industrien entscheidend. Sie können als freiwillige Referenz auch in Nicht-Finanz-Regulierungen eingearbeitet werden.

Auch wenn die Finanzkrise 2008 Anlass zur kritischen Hinterfragung der Risikomanagementsysteme von Finanzinstituten gab, werden aus diesem Bereich weiterhin fortschrittliche Regeln und Methoden mit breitem Anwendungsinteresse entwickelt werden.

Daher entspricht es gängiger Industriepraxis, sich methodische Inspiration und personelle Experten von der Finanzbranche zu holen. Welche Praktiken für Industrieunternehmen Sinn ergeben, muss als erster Schritt ermittelt werden. Klarheit über Unterschiede der eigenen Branche gegenüber Finanzunternehmen ist nötig, bevor ein solcher branchenübergreifender Transfer Früchte tragen kann. Zwischen einzelnen Branchen und sogar Unternehmen können beträchtliche Unterschiede von Möglichkeiten (Daten und IT), Herausforderungen der Branche, Bedürfnissen (Gesetze und Unternehmensleitung), Berufsalltag (Governance, Risikoappetit und Geschäftsnatur) oder sogar in der Kommunikation (Sprache und gelebtes Reporting) bestehen [McNish(März 2013), vgl. S.1].

Eine genauere Betrachtung welche bewährte Risikomanagementmethoden aus welchen Bereichen verwendet werden sollten, werden in Abschnitt 4.9 behandelt.

Risiko als Bewertungskriterium von Cooperate-Ratings

Übersicht über das Risikomanagement in Bezug auf Rating :

- Die Verwendung von Ratings im Risikomanagement unterliegt bei Industrieunternehmen keinen gesetzlichen Bestimmungen und ist freiwillig. Ratings können in die Frühwarnsysteme eingebaut werden [Gleissner(2011), S.286].
- Die zunehmende wirtschaftliche Bedeutung von Ratings liegt am Umstand, dass bei risikobehafteten Geschäften, z.B. im Anlagenbau oder Projektgeschäft, das Rating direkt die Finanzierungskosten bestimmt. Beim Rating helfen gute Bewertungen des Corporate Governance und Risikomanagements.
- Für Strategieentwicklung ist die Finanzierbarkeit der Kapitalkosten entscheidend und somit abhängig von der eigenen Ratingklasse. Die Folgewirkungen bei Nichtbeachtung des eigenen Ratings können die komplette Unternehmensstrategie beeinflussen [Denk(2008), S.198].
- Eine Ratingstrategie kann sowohl für die Risikobeurteilung als auch Finanzierung sinnvoll sein [Gleissner(2011), Abb. 93].

Die Überprüfung der Bonität eines Kunden oder Lieferanten erfordert viel Zeit, Daten, Erfahrung und somit Kosten. In der Praxis überbrücken die Dienstleistungen der Ratingagenturen die Informations-Asymmetrien zwischen Schuldner und Kreditgeber. Durch die einfache Zugänglichkeit und hohe Qualität ist es gängige Praxis im Risikomanagement, die

Risikobeurteilung anhand externer Ratings durchzuführen, vgl. [Pape(2011), S.173]. International auf den Kapitalmärkten sind vor allem die großen drei angloamerikanischen Ratingagenturen Standard & Poor, Moody und Fitch Rating zu nennen. National können Ratings auch von Versicherungen oder Kreditschutzverbänden (KSV) stammen, diesen Service gibt es für nahezu jede im österreichischen Firmenbuch eingetragene Kapitalgesellschaft [Denk(2008), vgl. S.199].

Das Rating eines Unternehmens beschreibt die Ausfallwahrscheinlichkeit (engl. Probability of Default), die weitestgehend mit der Insolvenzwahrscheinlichkeit (=Wahrscheinlichkeit der Überschuldung oder Illiquidität) übereinstimmt [Gleissner(2011), S.283]. Die Ratingklassen haben je nach Ratingunternehmen verschiedene Buchstaben-Zahlen-Kombinationen und reichen von der besten Kreditqualität (AAA, Aaa) über spekulative Kreditqualität (BB+, Ba1) bis zu starker Insolvenzgefährdung (C, Ca) [Pape(2011), S.173]. Letztlich gibt jede Ratingklasse einen Promillbereich an Insolvenzwahrscheinlichkeit an.

Allgemein umfasst die Beurteilung von Ratings [Gleissner(2011), S.283] :

- Das im Mittel erwartete Ertragsniveau und das Risiko, dass dieses davon abweicht,
- Risikotragfähigkeit (Eigenkapital und Liquiditätsreserven),
- Transparenz und Glaubwürdigkeit des Unternehmens aus Sicht der Kreditinstitute

Unternehmensratings (engl. corporate ratings) beinhalten finanzielle Kriterien, wie Cashflow, Schuldenhebel (engl. Leverage) oder Gewinn. Auch nicht-finanzielle Kriterien werden von Ratingagenturen mit bewertet. Sie beurteilen bei jedem Unternehmen die spezifischen Länderrisiken, Branchenrisiken und Marktposition. Auch deren Risikomanagement, Ressourcenabhängigkeit oder Operationseffizienz werden betrachtet [25]

Nötige finanztechnische Grundlagen im Risikomanagement

Klassische Literatur des Risikomanagements geht auf die finanztechnischen Grundlagen kaum bis gar nicht ein. Daher wird im folgenden Kapitel ein minimales Grundverständnis und weiterführende Literatur erläutert.

Betriebswirtschaftliche Kennzahlensysteme

Die industrieüblichen Finanzkennzahlen (engl. KPI für key-performance-indicator) können auf unterschiedlichste Weise definiert werden. In dieser Arbeit werden sie wegen der Nähe zum Risikomanagement aus den grundsätzlichen Aufgaben und Zielen des Controlling abgeleitet. Auf die Vielzahl der bekannten Kennzahlensysteme wird hier im Folgenden nicht eingegangen, das älteste Kennzahlensystem von DuPont aus dem Jahre 1919 kann als Anfangspunkt für detailliertere Betrachtungen dienen [Röhrenbacher(2008), S.335].

[25] http://www.standardandpoors.com/en_EU/web/guest/ratings/ratings-criteria/ und http://www.spratings.com/documents/20184/774196/Corporate+Ratings+Methodology.pdf/8fd4392a-4aae-4669-bd74-a9b86e18d781 (10.01.2015).

Eine grobe Einteilung kann in Erfolgs-, Liquiditäts-, Rentabilitäts-, Kapitalstruktur-, oder Umschlagshäufigkeitskennzahlen erfolgen [Vollmuth and Zwettler(2013), S.104ff]. Zu den wichtigsten Kennzahlen der Planung gehören [Vollmuth and Zwettler(2013), S.31]:

- Wirtschaftlichkeit (Rentabilität) anhand entweder Umsatzerlöse in der Bilanz oder der Aufwende in der GuV
- Shareholder Value (wertorientierte Steuerung) z.B. als Wirtschaftlichkeit anhand Kosten- und Leistungsrechnung
- Zahlungsfähigkeit (Liquidität) anhand der Ein- und Auszahlungen in der Liquiditätsplanung und des Cashflow aus dem operativen Geschäft. Oder anhand der Einnahmen und Ausgaben in der Finanzplanung.
- Ratingausblick als Finanzierungsgrundlage für Fremd- und Eigenkapital.

Diese klassischen finanziellen Unternehmensziele wie Wertsteigerungen, Umsatzwachstum, ausreichender Cashflow, Umsatzrentabilität, ausreichende Liquidität und Wirtschaftlichkeit können auch direkt als Ziele des Risikomanagements abgeleitet werden [Romeike and Hager(2009a), S.116].

Sehr oft hängen die vom Unternehmen gewählten betrieblichen Kennzahlen einerseits von den geltenden Rechnungslegungsvorschriften ab, z.B. Jahresabschlüsse siehe Abschnitt 2.4. Anderseits wählt man in der Praxis oft ein Kennzahlensystem nach den Analysezielen, Präferenzen und Erfahrungen der Nutzer aus.

Die Verlässlichkeit, Aussagekraft, Entwicklungstrends oder der Gesamteindruck über die Unternehmenslage sind nur so gut wie das Kennzahlensystem selbst. Die generelle Empfehlung lautet daher mehrere Kennzahlen über mehrere Geschäftsjahre zu betrachten und eine individuelle Methodik bei Einhaltung der Rechnungslegungsvorschriften zu entwickeln. [Pape(2011), S.282]

Die Grenzen von Kennzahlen werden am besten durch ihre Vor- und Nachteile beschrieben.

+ Die Vorteile von Kennzahlen sind ihre verdichteten Aussagen für einen schnellen Überblick des Unternehmens.

− Die Nachteile liegen in der Natur der Sache. Durch die Verdichtung können entscheidende Informationen verloren gehen, das notwendige Datenmaterial für die jeweilige Kennzahl muss ggf. aufgearbeitet werden. Des Weiteren ist es immer ein ex-post Blick in die Vergangenheit und die uneinheitlichen Definitionen der meisten Kennzahlen wirken erschwerend [Brösel(2004), S.578].

Die Kennzahlen sind auch in der Risikoforschung von Bedeutung und werden in Abschnitt 3.7 wieder aufgenommen.

2.5 Geschichte des Risikomanagements und der Risikoberechnung

Dieses Kapitel dient einerseits dem tieferen Verständnis und zeigt andererseits wie etabliert alte Risikotraditionen in vielen Bereichen und Branchen sind [McNeil et al.(2015)McNeil, Frey, and Embrechts, Kp. 1.2]. Man betrachte historische Unternehmensimperien, deren Überleben oder Untergang. Ursachen wie Technologiewandel, Marktblasen, Naturkatastrophen, Betrug oder schleichender Verlust der Konkurrenzfähigkeit. Dabei liegt der Schluss nahe, von einer ewigen Renaissance des Risikomanagements zu sprechen [Diederichs(2012), S.1], da spektakuläre Pleiten oder Skandale nie ein Ende nehmen. Risiken trugen sowohl die überlebenden wie verfallenen Unternehmensimperien, der Unterschied lag im Management. Um aus vergangenen Fehlern und Erfolgen Lehren für sich selbst ziehen zu können, findet sich im folgenden Kapitel eine geschichtliche Betrachtung.

Historisch betrachtet finden sich die Wurzeln des Risikomanagements im Arbeitnehmerschutz der handwerklich bzw. industriellen Fertigung (engl. Healthy, Safety and Environment, kurz HSE) und im frühen Handel und Bankwesen, welches mit Ausfallrisiken aller Art konfrontiert war, z.B. Naturkatastrophen oder menschlicher Verbrechen.

Das Glücksspiel ist ebenfalls als enger gedanklicher Vorreiter einer Risikobetrachtung anzusehen, denn es erschloss die Wissenschaft der Statistik und insbesondere der Stochastik (Wahrscheinlichkeitsbetrachtung). Letztlich bedurfte es einer Abwendung vom gläubigen Gottesschicksal während der neuzeitlichen Aufklärung, um die Entwicklung des wissenschaftlichen Risikomanagements in heutiger Form zu ermöglichen, [Romeike and Hager(2013), vgl. S. 9].

Beim Blick in die nähere Vergangenheit der letzten Jahrzehnte, zeigen sich vor allem zwei Entwicklungen, die die heutige Behandlung von Risiken veränderten. Riesige Datensammlungen und billige Computer-Rechenleistung ermöglichten die Entstehung eines auf Risikomaße (Kennzahlen) basierenden und automatisierten Risikomanagements [Damodaran(2008), S.65ff] und [McNeil et al.(2015)McNeil, Frey, and Embrechts, S.10] .

Weiters ist nach Raz und Hiller [Raz and Hillson(2005), vgl. S.53] in den Jahren vor dem Jahrtausendwechsel ein starker Entwicklungsschub bei den Methoden, IT-Tools, Prozessen und Theorien des Risikomanagement eingetreten. Dieser brachte das Risikomanagement weg von der simplen Einzelbetrachtung reiner Finanzrisiken oder operativer Sicherheitsrisiken, hin zu einer Gesamtbetrachtung aller Unternehmensbereiche. Dabei ziehen sie parallelen auf das geopolitische Wirtschaftsumfeld und die Veränderungen bei Informationstechnologie, Globalisierung, Outsourcing von Produktion, steigende Bürotätigkeiten, internationale virtuelle Teams, steigende Anzahl an Stakeholdern, steigende Regulierungen, Etablierung der Corporate Governance, steigender Konkurrenzdruck oder die generell steigende Komplexität international agierender Unternehmen.

Dieser Trend hielt in den folgenden 10 Jahren bis Heute an und intensivierte sich zusätzlich um die unternehmensweiten Komponenten einer integrativen IT-Plattform und Risikomanagement auf allen Ebenen. Alle diese Punkte sprachen und sprechen in den letzten

und kommenden Jahrzehnten für eine steigende Bedeutung und Ausbau des Risikomanagements [McNish(März 2013), S.1ff].

In den folgenden beiden Unterkapiteln, werden im Abschnitt 2.5 als erstes die Meilensteine der für diese Arbeit entscheidenden Risikoberechnung wiedergegeben. Denn erst durch die Quantifizierung mittels Risikomaß wird ein moderner Reifegrad im Risikomanagement erreicht. Als Abschluss wird im Abschnitt 2.6 die Geschichte des unternehmensweiten Risikomanagement aufbereitet, in Form von deren gesetzlichen Normungen und privaten Regelungsinitiativen.

Geschichtlicher Verlauf der Risikoberechnung

Die wichtigsten Entwicklungen bei den Risikomaßen gehen von der Entwicklung der Statistik als Erklärung des Glücksspiels, über erste Datenanalysen für Risikoabschätzungen in Versicherungsunternehmen, bis hin zu Risiko- und Chancenmaße für die modernen Finanzmärkte. Die einzelnen Entwicklungsschritte dienen dem besseren Verständnis, sowohl des Vokabulars, als auch der Limitationen und Möglichkeiten der teils immer noch in Verwendung befindlichen Risikomaße.

Risikoberechnung mittels statistischen Methoden

Durch die folgenden Entdeckungen wurde es möglich, die Wahrscheinlichkeiten von Ereignissen zu berechnen, nicht nur von ersten einfachen echten Zufallsexperimenten wie dem Münzwurf, sondern auch von jenen Ereignissen die mit komplexeren Unsicherheiten verbunden sind [Damodaran(2008), S.87].

- Bereits de Moivre berechnete 1712 mittels Losen in “de Mensura Sortis”, dass das Risiko, eine Summe zu verlieren, die Kehrseite der Erwartung ist. Ihr wahres Maß sei das Produkt der gewagten Summe multipliziert mit der Wahrscheinlichkeit des Verlustes.
- Das Bernoullische Gesetz der großen Zahlen machte es möglich von kleineren Stichproben auf die Grundgesamtheit zu schließen, bei mit dem Probenumfang steigender Genauigkeit. Eine Notwendigkeit für das Versicherungswesen. So fasste Jakob Bernoulli 1713 in “Ars Conjectandi”, die Stochastik nicht nur als Glückspielberechnung auf, sondern als Kunst der Vermutung.
- Die Normalverteilung durch Gauss, de Moivre und Laplace ermöglichte und verband Wahrscheinlichkeitsaussagen mit dem Durchschnitt und Standardabweichung des Probeumfangs.
- Baye’s “Gesetz der bedingten Wahrscheinlichkeiten” erlaubte es bereits bekannte Wahrscheinlichkeiten mit eintreffen neuer Informationen zu aktualisieren.

Die hier geschaffenen Grundlagen waren Ausgangspunkt für die finanzmathematischen Modelle und deren Anwendungen in der heutigen Wirtschaft [Romeike and Hager(2013), S.28ff], wie auf den folgenden Seiten beschrieben.

Risikoberechnung für die Finanzwirtschaft der Nachkriegszeit

Die in dieser Arbeit untersuchten Risikomaße insbesondere für Industrieunternehmen, bedienen sich der Erfahrungen und Best-practices aus dem für das Risikomanagement seit jeher als Vorreiter identifizierten Finanz- und Versicherungswesen.

Die Anfänge der Versicherung reichen weit zurück. Sie können in den Schiffsversicherungen der Phönizier, den Begräbnisvereinen armer Bürger im antiken Ägypten und Rom, aber auch in den bereits dort auftretenden Schiffsversicherungen gefunden werden. Im deutschsprachigen Raum zum Beispiel, verpflichtete Karl der Große um 700 n.Chr. Gilden zur gegenseitigen Hilfeleistung bei Krankheit, Verwittwung oder Alter. Diese Tradition hielt sich während des restlichen Mittelalters in den Zünften fort. Durch die 1590/91 beginnenden Seeversicherungen und Brandgilden in Hamburg wurde das deutsche Versicherungswesen etabliert [Romeike and Hager(2013), S.9ff].

Die Nutzung von historischen Datenansammlungen und Berechnungen von Erwartungswerten läutete die Zeit der Datenanalyse endgültig ein, siehe die wichtigsten Meilensteine [Damodaran(2008), Figure 4.5] und [McNeil et al.(2015)McNeil, Frey, and Embrechts, S.9]:

- Wichtige moderne Versicherungsgeschäfte sind die in London 1680 gegründete Feuerversicherung von Nicholas Barbondie. Das 1688 ebenfalls in London gegründete Lloyd's Coffee House mit Schiffsversicherungen und die von Edmond Halley 1693 gegründete Lebensversicherungsmathematik. Sie alle machten sich zunutze, dass Versicherungen die Wahrscheinlichkeit und erwartende Ausfallhöhe (expected loss) relativ genau anhand historischer Daten berechnen können.

- Die Investoren der frühen Finanzprodukte des 19. Jahrhundert waren es nun, die Risikomaße nicht nur als potentielle Verlustquellen sahen (Versicherungssicht), sondern auch deren Gewinnpotential zu berechnen versuchten. Dies wurde bewerkstelligt, indem ähnliche Gruppen von Finanzprodukten mit dem gleichem Risikolevel bewertet wurden. Dies geschah für risikoaverse (=risikoscheue) Investoren unabhängig von den Dividendenerwartungen, sondern mit der einfachen Heuristik ob es sich um eine alteingesessene Firma mit Reputation oder einer neu gegründeten handelte.

- 1909 wandten die Vorläufer der Ratingagenturen statistische Methoden auf die Informationen aus dem Rechnungswesen von Unternehmen an.

- Louis Bachelier leitete 1900 mit seiner Doktorarbeit über den Pariser Aktienmarkt, Modelle wie den random walk ein. Bachelier beinhaltet bereits das Optionsbewertungsmodell (put und call), Ansätze zum Capital Asset Pricing Model (CAPM) und die Portfoliotheorie, lange bevor diese von respektive Black, Scholes, Merton, Sharpe oder Markowitz veröffentlicht wurden.

- 1952 legte Markowitz mit seiner Portfoliotheorie den Grundstein für eine Portfolio Selektion nach risikogewichteten Gewinnen (engl. risk-return) und somit den Durchbruch der mathematischen Finanz. Damit wurden auch Derivate als Risikomanagement und

Spekulationsmethode beliebt. Derivate sind vertragliche Finanzinstrument die einem Asset eine zeitlich vereinbarte Option einräumen [McNeil et al.(2015)McNeil, Frey, and Embrechts, S.8-9]. CAPM ist umstritten, wegen den beobachteten fat tails, Asymmetrien und Preissprünge (Wahrscheinlichkeit und Auswirkung) die so nicht ins Modell reinpassen [Damodaran(2008), S.79-82].

- Die Subprime Krise 2007-2009 zeigte auch das Risiko von überzogenen Finanzmodellen und operative Risiken durch betrugsähnliche Gier. Hochriskante Assets wie kaum besicherte Konsumentenkredite erhielten bei Bündelung trotzdem Rating-Bestnoten und wurden mit Ausfallversicherungen mehrmalig weiterverkauft. Bis schließlich diese “magic-of-securitization” Blase platzte [McNeil et al.(2015)McNeil, Frey, and Embrechts, S.11-14].

Eine Auflistung aktueller Risikomaße und -modelle finden sich im Kapitel Abschnitt 3.7 .

Das angloamerikanische ALARP Prinzip

Oft werden die residual-risk (dt. Restrisiko) in den angloamerikanischen Normen erwähnt. Diese stehen eng im Zusammenhang mit den tolerable-risk (dt tolerierbare Risiken) und dem ALARP-Prinzip (engl. as-low-as-reasonably-practicable), siehe die Norm AS-NZS 4360 Kapitel 7.4. Restrisiko ist das Risiko, das nach der Risikosteuerung der ursprünglichen Risikohöhe durch Maßnahmen verbleibt.

Der Report des “Robens Committee of Inquiry” bezüglich “Health and safety”, brachte 1972 in Großbritannien Reformen rund um die Gesundheit und Sicherheit auf. Hohe Zahlen von “Incidences and accidents and ill health”-Fällen durch den rasanten technischen Fortschritt begründeten die Notwendigkeit. Industrielle Unfälle mit teilweise ungeschützter Öffentlichkeit häuften sich. Bekanntester Fall war der Chemieunfall im Jahr 1976 in Seveso, Italien. Während seiner Klärung entstanden diverse Regelungen wie die erste funktionale Sicherheitsnorm EN 61408 oder eben jenes Committee von Robens.

Europaweit wurde die Art der gesetzlichen Regelungen überdacht und ein Paradigmenwechsel vollzogen. Weg von detaillierten Gesetzen je Branche, hin zu generischen, branchenübergreifenden Regelungen [Bouder and Slavin(2013), S.90-93]:

- Die Hauptverantwortung für die Kontrolle liegt bei jenen, die die Risiken erschaffen
- Die Legislatur erschafft Rahmen zur Selbstregulierung und damit Wahlfreiheit beim Lösungsansatz, solange die Sicherheitsziele erreicht werden
- Die Industrie soll eine aktive Rolle bei der Entwicklung von Standards und Richtlinien einnehmen, anhand von best-practice Beispielen?
- Health and Safety soll ein normaler Bestandteil des Managements sein

Durch diese Sicherheitsphilosophie der Legislative können aus Sicht des Gesetzgebers Risiken sicher genug gemacht werden (engl. “as low as reasonable practicable”). Die regulative Hauptbetrachtung des ALARP liegt darin, Umfang und Notwendigkeit einer Risikoreduktion zu untersuchen. Bei “high-hazard-industries” muss das umso intensiver erfolgen.

“The overriding consideration is that safety must be given the benefit of any doubt, whether the doubt refers to the applicability of good practice or the treatment of uncertainties in analysing options for reducing the risks. [...] where risk are high, the balance in favour of safety must be substantial [Bouder and Slavin(2013), S.90-93].”

Aufbauend darauf schlug 1987 Sir Frank Layfield während des Baus des Sizewell B Atomreaktors bei einem Report vor, tolerierbare Risikogrenzen für Individuen (Arbeiter) und die Gesellschaft auszuarbeiten. Daraus entstand 1992 ToR (Tolerability of Risk framework). ToR wurde in weiterer Folge als Vorlage für andere Branchen für die Risiko-Entscheidungsfindung (engl. risk-decision-making) genutzt [Bouder and Slavin(2013), Kp.4].

2.6 Geschichtlicher Verlauf der Risikomanagement Normung

Im Normwesen findet man die Tradition vor, dass generische Normen, sogenannte Mutternormen, eine allgemeine begriffliche Basis und theoretisches Fundament der Grundprinzipien aufbauen und dann mittels abgeleiteten Tochternormen branchenspezifischen Eigenheiten Rechnung tragen. Nach diesem Schema wurden auch die technischen Sicherheitsnormen aufgegliedert. Am Beispiel der funktionalen Sicherheit erläutert, so gilt im technischen Risikomanagement die generische DIN EN 61508 für die Funktionale Sicherheit aller Bereiche, doch aus ihr resultierten Normen für medizinische Geräte (DIN IEC 60601), Fahrzeugbau (DIN ISO 26262), Bahnbau (DIN EN 50100ff), Kernkraftwerke (DIN IEC 61513), Prozessindustrie (DIN IEC 61511) oder Maschinenbau (DIN EC 62061) vgl. [Löw et al.(2010)Löw, Pabst, and Petry, S.17].

Das Risikomanagement als Managementdisziplin und unter Einbeziehung von organisatorischen und methodischen Vorgaben wurde auch für Industrieunternehmen in den späten 1990er Jahren zunehmend zur Verpflichtung.

- NS5814:1991 Requirements for risk analyses
- AS/NZS 4360: 1995 Risk management
- CAN/CSA Q850:1997 Risk Management: Guideline for Decision-Maker
- IEC 62198:2001 Managing risk in projects - Application guidelines
- Sarbanes-Oxley-Act 2002
- COSO II: 2004 Enterprise Risk Management
- ISO 31000:2009 Risikomanagement Grundsätze und Leitlinien
- ONR 4900X:2010 Risikomanagement für Organisationen und Systeme

Die erste risikonahe Norm war die norwegische Norm NS5814 im Jahre 1991, jedoch beschränkte sie sich auf Risikoanalyse und behandelte keine Regelkreise wie jene des RM-Prozesses noch den RM-Rahmen vgl. [Raz and Hillson(2005), S.54].

Die australische Risikomanagement Norm AS/NZS 4360 behandelte als erste einschlägige Norm das Risiko als Managementthema und mittels Regelkreis im RM-Prozess. Verglichen mit der ein paar Jahre später entwickelten kanadischen Risikomanagement Norm Q850 stechen sowohl andere Schwerpunkte mit Managementphilosophien, als auch noch ein unterschiedlicher Aufbau ohne Regelkreis hervor. Beide frühe Normen legen Fokus auf den Prozess und populärwissenschaftliche Sprache. Den zweiten Regelkreislauf RM-Rahmen, wie er später in ISO 31000 vorkommt, wird noch nicht explizit eingebaut. Die Themen des heutigen Rahmens wie initialer Kontext oder Risikophilosophie werden aber bereits erwähnt. Die Handbücher australisch/neuseeländisch HB 142:1999 und HB 143:1999 unterstützten bereits Unternehmen als Anwendungsleitfaden zur praktischen Industrieanwendung. Beides ist heute als "HB 436:2004 Riskmanagement Guidelines Companion to AS/NZS 4360" zusammengefasst. Ein wichtiger Hinweis bei der Behandlung dieser Normen sei gegeben durch die Abschnitt 2.3.

Bei den relevanten US-Standardwerken ist vor allem die 1985 gegründete Committee of Sponsoring Organizations of the Treadway Commission (COSO) als privatwirtschaftliche Organisation zur Verbesserung der Finanzberichterstattung zu nennen [DGR(2008), S.8]. Während sich der erste COSO Teil ausschließlich um die Gestaltung eines internen Kontrollsystems (IKS) kümmerte, befasste sich COSO II mit der Ausgestaltung eines Risikomanagementsystems, welches dort als Erweiterung des IKS aufgefasst wird.

Die im Kapitel Abschnitt 2.1 erwähnten Enron und WorldCom Skandale lösten die Einführung des Sarbanes-Oxley-Act 2002 für börsennotierte Unternehmen in den USA aus. Die Änderungen betrafen Corporate Governance, Finanzberichterstattung und interne Kontrolle und brachten höhere Mindestanforderungen und höhere Strafen [Denk(2008), S.52]. Diese hatten ähnliche Regulierungen weltweit zur Folge, so zum Beispiel den sogenannten "EURO-SOx" als Council Directive 2006/43/EC, den japanischen "J -SOx" 2007, den chinesischen "C-SOx" 2009, das österreichische Unternehmensrechtsänderungsgesetz (URÄG) 2009 oder das deutsche Bilanzrechtsmodernisierungsgesetz (BilMoG) 2010 [Racz(2011), S.16-17].

IEC entwickelte 2001 mit der "IEC 62198:2001 Managing risk in projects Application guidelines" eine Herangehensweise mittels Risikomanagement-Prozess-Regelkreis, welche der australischen Norm ähnelt, jedoch den engeren Projekt-Sinn hervorhebt. In der 2013 Ausgabe ist bereits eine Übersicht mit parallelen zur ISO 31000 enthalten.

Schließlich wurde die internationale ISO 31000 Norm federführend von den australisch/neuseeländischen und japanischen Normungsinstituten erarbeitet, sie basiert augenscheinlich auf den AS/NZS 4360. Die ONR 49000 ist wiederum die nationale Umsetzung der internationalen Norm und als solche beinhaltet sie selbstverständlich den kompletten ISO 31000 Umfang. Jedoch zeichnen die ONR vor allem die Folgebände aus, welche unter der Nummerierung ONR 49001,49002 und 49003 als umfangreiche Handbücher konzipiert wurden.

Abschließend wird in Tabelle 2.6, ohne detaillierte Ausarbeitung des historischen Verlaufs, eine Übersicht über gängige Normen und Leitlinien geben, mit speziellen Augenmerk auf deren Risikomanagement-Bestandteile.

Standard	Aufgabe	Branche	Risikorelevanz
COSO	Unternehmensweites Risikomanagement	alle	umfassende Risikoleitfaden
ISO 31000	Unternehmensweites Risikomanagement	alle	generische Risikonorm
Basel 3	Risikomanagement	Bank	Risikonorm, Aufsichts- und Eigenkapitalregeln
IFRS 6	internationale Rechnungslegung	alle	siehe Abschnitt 2.4
Solvency	Risikomanagement	Versicherung	Risikonorm, Aufsichts- und Eigenkapitalregeln
PMBOK Guide	Projektmanagement	alle	Kp. 11 Project Risk Management
pm baseline	Projektmanagement	alle	Kp.2.4.10 Projektrisiken und Kp.4 Projektportfoliorisiken
DIN 69901-2	Projektmanagement	alle	Risiko einbezogen
DIS ISO 9001:2014	Qualitätsmanagementsysteme	alle	Risiko neu dabei
EFQM	Total Quality Management	alle	Risikomanagement in Prozesslandschaft
COBIT	IT Governance	IT	EDM03, EDM05, APO12, MEA02, MEA03, DSS03; (Ähnlichkeit zu COSO)
ITIL bzw. ISO 20000-X	IT Service Management	IT	Business Continuity und Security Management Bestandteil
ISO 2700X	Information security management	IT	TEIL 27005 beinhaltet nur Risikomanagement
SWEBOK	Engineering Guidebook	IT	Ordnungsgemäßer Softwareentwicklung inkl. Risiko
SPICE	Reifegradmodelle	alle	Risikomanagement als Managementprozess 5
CMMI	Reifegradmodelle	alle	Ab Reifegrad 3 (von 5) ist RM nötig

Tabelle 2.4: Übersicht der Risikomanagement-Bestandteile in verschiedenen Normen

Abschließend ist wichtig darauf hinzuweisen, dass zusätzlich zu den oben erwähnten allgemein gültigen Risikonormen, viele Branchen eigene Risikomanagement-Bereiche aufweisen.

- Zum Beispiel sind in der IT allgemeine Vorschriften unter IT Governance (z.B. ISO 38500:2008, COBIT, ITIL), sowie IT- und Datensicherheit mittels der ISO 27000 Serie geregelt.

- Im Maschinenbau ist die funktionale Sicherheit mit der Mutternorm IEC/EN 61508 geregelt, dabei handelt es sich um eine Art des technischen Risikos bei elektrisch-elektronisch-programmierbaren Maschinen. Noch speziellere Bereiche haben eigene Tochternormen, so Kernkraftwerke die DIN 61513, Medizingeräte DIN 60601, Bahn

DIN 501xx oder PKWs ISO 26262.

2.7 Zusammenfassung über die Bedeutung des Risikomanagements

Die isolierte Betrachtung und Absicherung von Einzelrisiken verliert zusehends an Bedeutung und wird durch einen unternehmensweiten Risikomanagementansatz inklusive Interdependenzen und Maßnahmen ersetzt.

Zentrale Ansätze dieses unternehmensweiten Risikomanagements sind dabei:

- das ganzheitliche Management von Risiken,
- das Management aller betrieblichen Risiken,
- Berücksichtigung von Risikointerdependenzen
- die Integration des Risikomanagements in die Unternehmenssteuerung

Des Weiteren wird versucht das Risikomanagement in die Gesamtsteuerung des Unternehmens zu integrieren. Dies erfordert insbesondere die Integration von Risikozielen in die Unternehmensziele. vgl [Denk(2008), S.34].

Die Geschichte des modernen Risikomanagements macht deutlich, dass ihre Wurzeln in zwei Branchen zu finden sind, der Finanzwirtschaft und der funktionalen Sicherheit von Produkten. Im Risikomanagement der Finanzwelt werden Risikokennzahlen und -limiten in Operationelle-, Markt-, Kredit- und Liquiditätsrisiken unterteilt. In vielen anderen industrienahen Branchen sind die dafür nötigen Daten kaum existent und das dortige Risikomanagement heißt in der Finanzindustrie oftmals Risikocontrolling. Daher müssen Erfahrungswerte und deren Übertragung zwischen den verschiedenen Branchen mit Bedacht genutzt werden [Pergler(Dezember 2012), S.1ff] , siehe dazu Abschnitt 4.9.

Teil II

Unternehmensweite Risikomanagementsysteme in Theorie und Praxis

KAPITEL 3

Grundlagen für unternehmensweite Risikomanagementsysteme

3.1 Kapitelübersicht

Aufbauend auf die Grundlagen des Kapitel 2 wird in diesem Kapitel jeweils auf die aktuellen Methoden im Risikomanagementprozess und -rahmen detailliert eingegangen.

Im ganzen Kapitel 3 werden an die 100 Methoden vorgestellt. Viele davon sind für andere Zwecke oder Branchen entwickelt worden. Daher müssen Erfahrungswerte und deren Übertragung zwischen den verschiedenen Branchen mit Bedacht genutzt werden!

Ebenso mit Bedacht ist die Vielzahl an ähnlichen und redundanten Risikobegriffen zu verwenden, im Kapitel Abschnitt 3.3 werden sie säuberlich ausgearbeitet. Unter anderem finden sich detaillierte Beschreibungen von Zielen, Risikoappetit, Risikosituation, Risikomanagementpolitik, Risikophilosophie, Risikoleitsätzen, Risikomanagementstrategie, Risikokultur, Risikotransparenz und Reifegraden.

Das Risikomanagement besteht aus zwei PDCA-Regelkreisläufen, dem übergeordneten Risikomanagementrahmen und dem in allen Unternehmensbereichen verankerten Risikomanagementprozess.

Der Risikomanagementrahmen in Abschnitt 3.3 beschreibt den äußeren PDCA-Regelkreislauf. Für eine erfolgreiche Einführung bedeutet das ein nötiges Umfeld, Kultur, Leitbild, Ziele und Strategie im Unternehmen. Im regulären Betrieb regelt der Rahmen Grundlagen und Organisation für die Gestaltung, Umsetzung, Kommunikation, Überwachung, Überprüfung und kontinuierliche Verbesserung des Risikomanagements. Der Risikomanagementprozess definiert die unternehmensweite Innenansicht, wie Risiken zyklisch bearbeitet werden, von Identifikation über Bewertung bis hin zur Kontrolle.

Die Einbettung des Risikomanagements in die Organisation muss durch die Unternehmensführung sichergestellt werden. Sie erscheint für eine enge Verzahnung des Risiko-

managements in bestehende Managementsysteme, Prozesse und Strategieentwicklung für eine Erhöhung von Synergie und Benutzerfreundlichkeit, besonders empfehlenswert. Dafür werden 2 Modelle vorgeschlagen:

- Abbildung 3.1 zeigt ein selbstentwickeltes Modell zur Verknüpfung des Risikomanagements (Rahmen und Prozess) in die Unternehmenshierarchie. Dies wird durch aufeinander aufbauenden Kennzahlen erreicht, so dass ein quantifizierbares und gelebtes Risikomanagementsystem entsteht.

- Abbildung 3.4 zeigt das three-lines-of-defense Modell mit der mehrstufigen Rollenverteilung des Risikomanagements im Unternehmen und den dazugehörigen Verantwortlichkeiten. Die Verantwortlichkeiten können sowohl in organisatorische als auch risikokategorische Gesichtspunkte unterteilt werden. Mögliche Organisationsstrukturen und Schnittstellen zu artverwandten Abteilungen wie Qualitätsmanagement, interne Kontrolle, interne Revision oder in die Unternehmenssteuerung werden in Abschnitt 3.4 erörtert.

Der Risikomanagementprozess ab Abschnitt 3.5 beschreibt den inneren PDCA-Regelkreislauf. Dabei werden alle Komponenten des Risikomanagementprozesses als Prozessschritte in einem eigenen Unterkapitel beschrieben. Jedes Unterkapitel hat eine Zusammenfassung zu Beginn um Übersicht durch Definitionen, Kriterien, Ziele und Übergänge zum vorausgegangen und nachfolgenden Prozessschritt zu schaffen. Anschließend werden die verschiedenen Ansätze zur Lösung dieses Prozessschrittes erklärt. Danach folgt eine Auflistung und Erklärung aller möglichen Methoden die man für den jeweiligen Prozessschritt nach subjektiven Präferenzen wählen kann. Abschließend werden Spezialthemen aus diesem Prozessschritt im Detail behandelt.

Hervorzuhebende Spezialthemen:

- Die Risikoidentifikation in Abschnitt 3.6 beschreibt seltene Spezialrisiken und die Kategorisierung der Risiken.

- Bei der Risikobewertung sind die Fragen nach der Risikoquantifizierung und - aggregation die Schwierigsten. Bei der Risikoquantifizierung geht es primär um eine nachvollziehbare und zuverlässige Abschätzung von Risiken. Der wesentliche Schritt der Risikoquantifizierung ist eine entsprechende Datenbasis, also die Messung von Daten und deren Datensammlung. Die Risikoquantifizierung in Abschnitt 3.7 geht auf die natürlichen Verteilungsfunktionen von Risiken in Abbildung 3.10 ein und auf das bekannte Risikomaß value-at-risk mit verschiedenen Berechnungsmethoden in Abbildung 3.12. Die Aggregierung von Risiken meint zwei Punkte, die gegenseitige Beeinflussung von Risiken in Form von Korrelationen und das Ergebnis einer Zusammenführung von Einzelrisiken als Gesamtrisiko des Unternehmens, einer Risikokategorie oder einem Unternehmensbereich.

- Die Risikosteuerung in Abschnitt 3.8 kann nach Abbildung 3.13 durch mehrere Maßnahmen erfolgen und hat je nach Risiko konkrete Maßnahmenvorschläge in Tabelle 3.6 aufgelistet. Prototypisch sind ein projektmanagementorientierter Maßnahmenplan in Tabelle 3.5 und eine Früherkennung mit umfangreicher Indikatorenliste in Tabelle 3.7 beschrieben.

- Die Risikokontrolle in Abschnitt 3.9 behandelt das aus Erfahrungen der internen Kontrolle übertragene Kontrollhebel Modell und eine Vorlage eines Verhaltens- und Ethikkodex.

- Spezialthemen zur Information, Kommunikation und Berichterstattung sind weitestgehend durch das prototypische Informationssystem in Abschnitt 4.5 beschrieben.

- Die Überwachung in Abschnitt 3.11 wird durch Überprüfungsfragen der Compliance ergänzt.

Hervorzuhebende Ansätze:

- Zur Risikoidentifikation kann der bottom-up oder top-down Ansatz dienen, letzterer ohne breiträumige Einbindung der Angestellten.

- Die Risikobewertung kann grundsätzlich mit Hilfe qualitativer und quantitativer Maße oder Bewertungsskalen erfolgen. Beispiele für das Erste sind Expertenschätzungen und für das Zweite die Nutzung von Verteilungsfunktionen.

- Gängige Ansätze der Risikosteuerung reichen von einer Risikolimitierung durch Vorgaben mittels Kennzahlen, einem Projektmanagementzugang bis hin zur Verhinderung durch Frühindikatoren.

- In ihrem Ansatz kann man manuelle oder automatisierbare, präventive oder detektive, primäre oder sekundäre und routinemäßige oder außerplanmäßige Risikokontrollen unterteilen.

Abschließend noch zwei anregende Metapher aus der Praxis:

> “Die Projekte, die es Wert sind gemacht zu werden, werden in der Risikobewertung negativ bewertet [Marco and Lister(1987), S. 189]!”

> “Die Verbindung zwischen Risiko und Gewinn wird oft erwähnt aber ebenso wichtig ist auch die Verbindung zwischen Risiko und Risikobewusstsein. Denn Risiken einzugehen ist nicht automatisch gefährlich, gefährlich wird es erst durch die Ignoranz der Konsequenzen. Ein Risikomanagementrahmen entwickelt genau dieses Risikobewusstsein, bis hin zur Natur und Bedeutung der größten Risiken [Simons(1999)].”

3.2 Die Konzeption eines Risikomanagementhandbuch als Einstieg zum Thema

Die vielerorts als Formalisierung und Unternehmensrichtlinie herausgegebenen Risikomanagementhandbücher können als Teil der Organisationsrichtlinien gelten, daher sind sie wichtig. Insbesondere sollen Risikomanagementhandbücher für den operativen Betrieb, das Konzept des Risikoprozesses, die Grundsätze des Risikomanagementrahmen und die strategischen Zielvorgaben zusammenfassen [MaRisk(2014), S. 61]. Dies kann soweit führen, dass alle Richtlinien die das Risikomanagementsystem betreffen zusammen das Handbuch bilden. In dieser Arbeit wird eine übersichtliche Zusammenfassung, mit Verweise auf vertiefende Dokumente, bevorzugt, siehe Abschnitt 4.8.

Für durchschnittliche Nutzer ist das Risikomanagement meist nicht intuitiv nutzbar. Es sollten im Handbuch Grundlagen für ein gemeinsames Verständnis beschrieben werden, die von der Erklärung der Begriffe, grundsätzlichen Annahmen, bis zu den gesetzlichen Pflichten reichen. Die finale Ausgestaltung des Handbuchs ist firmenspezifisch, weitere typische Inhalte sind nach [Gleissner(2011), S. 219] :

- Risikopolitische Grundsätze des Unternehmen, welche im Einklang mit der Unternehmensstrategie stehen. Daraus wird die Risikostrategie abgeleitet.
- Verbindliche Dokumentation und Regelung der Aufbau- und Ablauforganisation, der Verantwortlichen und der Prozessschritte des kompletten Risikomanagements.
- Erklärungen von Methoden, Werkzeugen und Verfahren mittels Musterbeispielen und -berichten.
- Risikotragfähigkeit, als die Festsetzung der Limiten und des Risikoappetits als Akzeptanz der Risiken.

Begriffe wie Risikokultur, -philosophie, -politik, -leitsätze, oder - strategie werden häufig in der Unternehmenspraxis genannt und sind in ihrem Inhalt teilredudant und unscharf. Die Begriffe sind meist nur im Zusammenhang des jeweilig verwendeten Modells eindeutig und können erst bei Betrachtung ihrer einzelnen Bestandteile unterschieden werden. Zusammenfassend sind Risikobegriffe meist aus der hochspezialisierten Sicherheitstechnik oder der normalen Managementsprache, wie Organisationsform, Ziele, Strategie, Planung, Hierarchie, etc., entnommen und damit immer mit Bedacht auf die Situation zu nutzen.

Auch das Risikomanagement als wissenschaftliche Disziplin hat noch keine eindeutig definierte Terminologie. Die wichtigsten Begriffe und ihre Perspektive sind weder genau geklärt, noch überschneidungslos sondern eher von vielen Seiten bunt vermischt. Die langfristige Bedeutung dieser Disziplin als abhängige oder eigenständige Managementdisziplin bleibt abzuwarten. Offen ist auch, ob es als Trendthema für Unternehmen wieder verschwindet und in die etablierte Rolle, als Kernfunktion der Finanzbranche, zurückkehrt.

Zusätzlich kommen im Fachjargon der diversen Standardwerke, Journale und Beratungsfirmen weitere unscharfe Verwendungen hinzu. Dies kann nur durch Festlegung auf ein einziges der Beispiel-Begriffsmodelle und gewissenhafter Abklärung im eigenen Risikomanagementhandbuch vermieden werden, siehe Abschnitt 4.2. Im Zweifelsfall können die Begriffe aus dem Glossar von [ISO(2009), S. 8ff] oder der mehrsprachigem [ONR(2014a), S. 5ff] entnommen werden.

Die in dieser Arbeit gewählten Begriffe und ihr Zusammenhang im Unternehmen sind in Abbildung 3.1 sichtbar.

Eine anschauliche Klärung der Unterschiede zwischen den Begriffen, kann am folgenden Beispiel einer Risikobeschreibung veranschaulicht werden:

$Das\ ist$ Beschreibung des Sachverhaltes, der eintreten könnte und dann Ursache für einen Schaden wäre!

$+$ Bei jedem achten Zugriff auf die Bankkarte wird das Zertifikat nicht richtig ausgelesen, der Kunde kann kein Geld abheben.

$Das\ ist\ nicht$ Beschreibung des Schadens.

$-$ Kunde will Schadensersatz, weil er kein Geld bekommt.

Da das Risikomanagement etlichen angloamerikanischen Einflüssen unterliegt, ist auch auf sogenannte sprachliche “falsche Freunde” zu achten. Begriffe die zwar im Deutschen und Englischen ähnlich geschrieben sind aber eine andere Bedeutung haben. Beispiele hierfür wären Kontrolle (dt.) das nicht Controlling (engl.) entspricht oder level or risk (engl. für Risikohöhe). Es gibt auch Fälle in denen es keine passende deutsche Übersetzung gibt, beispielsweise bei Sicherheit (dt.). Im deutschen hat das Wort eine überlappende Bedeutung, im englischen gibt es mit Safety (engl.) für z.B. Arbeitssicherheit und Security (engl.) für z.B. Datensicherheit zwei spezifischere Wörter.

Das anschließende komplette Kapitel Kapitel 3 vermittelt die Theorie zum Aufbau eines Risikomanagement und passendem Handbuch. In der Praxis wurde dies in Abschnitt 4.8 umgesetzt.

3.3 Grundlagen des Risikomanagementrahmen

Der Risikomanagementrahmen nach ISO 31000, siehe Abschnitt 2.2, regelt Grundlagen und Organisation für die Gestaltung, Umsetzung, Kommunikation, Überwachung, Überprüfung und kontinuierliche Verbesserung des Risikomanagements. Für Unternehmen sind somit nach [ISO(2009), Kp.4.3] folgende Aufgaben zu erfüllen:

- Verständnis der eigenen Organisation und ihrer Zusammenhänge
- Festlegung der Risikomanagementpolitik
- Regelung der Verantwortlichkeiten

- Integration des Risikomanagements in die Prozesse
- Bereitstellung der nötigen Ressourcen
- Aufbau der internen und externen Risiko-Kommunikation und passender Berichterstattung
- Überwachung und ständige Verbesserung des Risikomanagementrahmens

Durch die aufgezählten Punkte sieht man, dass die Vorbildfunktion der Geschäftsführung durch das sogenannte tone-of-the-top für die erfolgreiche Einführung eines Risikomanagementsystems wichtig ist. Nur dort kann die Notwendigkeit und Priorisierung erfolgen. Dies wird in der ISO 31000 [ISO(2009), Kp.4.2] als Mandat und Verpflichtung aufgelistet und im zunehmenden Maße gesetzlich gefordert, siehe Abschnitt 2.2.

In ähnlicher Weise definiert dies der COSO II ERM Standard [COSO(2009a), S. 27ff] im internen Umfeld und unterstreicht, dass ohne dem richtigen Umfeld im Unternehmen kein Risikomanagementsystem Erfolg haben kann. Es muss seitens der Mitarbeiter spürbar sein, dass sie mit Übernahme der Risikoverantwortung auch verantwortlich gemacht werden. Nicht für Schadenseintritt, sondern nur für unterbliebene Risikomeldung, siehe Abschnitt 4.3. Mitarbeiter müssen den oftmaligen Kulturwandel annehmen und ihre Problemlösungen mit einer Risikoabschätzung kombinieren.

Zusammenfassend sind die Aufgaben eine Kombination aus Sicherheitsmanagement und betriebswirtschaftlicher Gestaltung und Optimierung. Das Top-Management muss als Erstes tatkräftig mitwirken und sein Interesse am Risikomanagement im ganzen Unternehmen spürbar machen. Wortreiche Bekenntnisse alleine reichen nicht. Erst dann kann durch einen periodischen plan-do-controll-act-circle (dt. Deming-Kreislauf) ein Wettbewerbsvorteil mit Risikomanagement und Risikokultur entstehen. Darüber verfügen nur wenige Unternehmen, aber nach Abschnitt 4.9 wird es gerade im dynamischen Marktumfeld allerseits gefordert!

Die hier aufgearbeiteten Theorien werden im Abschnitt 4.3 praktisch angewendet.

Zur Konzeption eines Risikomanagementsystems

Die Kombination des Risikomanagements aus Rahmen und Prozess mit dem Unternehmen, sodass ein quantifizierbares und gelebtes Risikomanagementsystem daraus wird, zeigt Abbildung 3.1. Dabei sieht man, dass das Risikomanagement mit 6 Komponenten, von Zielsetzung über internes Umfeld (durch Risikokultur ausgedrückt) bis Kontrolle, dargestellt wird. Alle Komponenten haben dazugehörige Risikokennzahlen, von Risikolimit bis Risikokapazität, welche wiederum mit den verschiedenen Hierarchien im Unternehmen, von den 3 line-of-defense bis zum Kapital, verknüpft sind. In Abbildung 3.1 verbindet das unternehmensweite Risikomanagement in seiner Natur einerseits einen Strategieprozess inklusive Change-Management und anderseits eine große Risikokalkulation.

Die Abbildung 3.1 und Abbildung 3.2 zeigen die Verknüpfung des Unternehmens mit dem Risikomanagementrahmen und -prozess. Die 6 Einzelschritte sind:

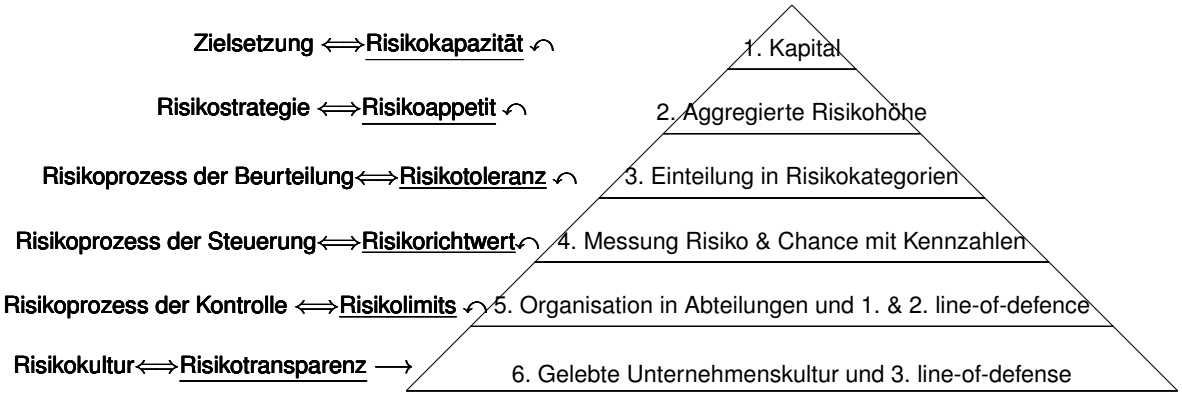


Abbildung 3.1: Verknüpfung des Risikomanagement in die Unternehmenshierarchie (grafisch als Pyramide dargestellt) [ERNST&YOUNGS(2010), vgl. Fig.1]

1. Die **Kapitalsituation** des Unternehmens stellt den Ausgangspunkt der Risikobetrachtung dar.

⟺ Ein Unternehmen richtet sich nach seinen Zielen aus. Nach diesen Zielen ist auch das Risiko zu bemessen. Die Risikoziele des Risikomanagement sind ebenfalls Teil dieser Zielen, nach Abschnitt 3.3.

↶ Die daraus entstehende Risikokapazität ist die quantifizierte Finanzpotenz, die ein Unternehmen an Verlusten maximal stemmen kann. Dabei sind die eigene Finanzstruktur und die kurzfristigen Finanzierungsmöglichkeiten zu beachten.

2. Die unternehmensweite **Aggregierung der Risiken** ist zur Ermittlung der Toprisiken und um zusammengefasste Unternehmensbereiche und -tätigkeiten beurteilen zu können wichtig, siehe Abschnitt 3.7. Dabei darf nicht vergessen werden, dass es sich um Schätzungen und Szenarien handelt, die noch von den Entscheidungen über Geschäfts- und Risikomaßnahmen des Unternehmens abhängen.

⟺ Die Risikopolitik liegt der Entscheidung der Unternehmensführung bezüglich Risikokapazität zu Grunde, Details siehe sec:Risikopolitik. Zusammen mit den Zielen wird hier aus der Risikopolitik eine Risikostrategie erstellt.

↶ Beim Vergleich zwischen Risikokapazität und aggregierten Risiken wird der tatsächliche Risikoappetit des Unternehmens auf der Führungsebene entschieden. Es ist der natürliche Balanceakt zwischen Geschäftschancen und -risiken und soll die Unternehmenskultur berücksichtigen.

3. Die **Risikokategorie** im Unternehmen ist eine wichtige Unterteilung der vielen Risiken in wenige aber dafür übersichtliche und relevante Risikobereiche. Diese Kategorien können separat Methoden und Experten zugeteilt werden und geben der Unternehmensleitung eine top-down Übersicht.

$\Longleftrightarrow$ Parallel zur Einteilung des laut Abschnitt 3.6 identifizierten Risikoinventars in Kategorien, findet der Prozess der Risikobeurteilung statt. Dabei werden anschließend laut Abschnitt 3.7 die Risiken im Detail analysiert und bewertet.

$\curvearrowleft$ Der Risikoappetit der Unternehmensleitung wird in diesem Schritt überschlagsmäßig mit einen Minimum und Maximum-Bereich auf die verschiedenen Risikokategorien und Unternehmensbereiche verteilt. Diese quantifizierten Grobvorgaben werden als Risikotoleranzen bezeichnet und dienen anschließend den Risikoeignern und der mittleren Führungsebene als Orientierung.

4. Die **Messung** der Risiken findet auf allen Unternehmensebenen statt und kann so unter Einbezug der vorgegebenen Risikotoleranz mit dem jeweiligen Businessplan und Kennzahlen von den Risikoeignern gesteuert werden.

$\Longleftrightarrow$ Diese Risikosteuerung unter Abschnitt 3.8 ist die aktive Veränderung des initialen Risikos durch Maßnahmen um schließlich ein akzeptables Restrisiko zu erhalten.

$\curvearrowleft$ Durch die Steuerung der Risiken entstehen verbindliche Entscheidungen der Risikoeigner, darüber welche Risikohöhe sie als passend ansehen. Dabei bedeutet passend, ein passendes Verhältnis zwischen den Gewinnchancen und Risikoverlusten. Diese geplanten Risikorichtwerte sind für die Kontrollprozesse und Unternehmenssteuerung relevant.

5. Die Risikorichtwerte werden von den Risikoeignern auf alle Prozesse in ihren **Organisationseinheiten** angewendet, sie sind die sogenannte 1. line-of-defence. Zusätzlich arbeiten sie bereits mit den Risikokontrolleinheiten, der 2. line-of-defence, zusammen. Siehe Abschnitt 3.4.

$\Longleftrightarrow$ Hier sind die Vorgaben des Überwachungs- bzw. Kontrollprozesses im Risikomanagement laut Abschnitt 3.10 zu beachten.

$\curvearrowleft$ Schließlich werden Risikolimits definiert, welche als risikospezifische KPIs (engl. Key Performance Indicators für Kennzahlen) auch im Informationssystem automatisiert überwacht werden können.

6. Das Risikomanagement muss in der gelebten **Unternehmenskultur** ankommen und diese positiv und schrittweise verändern. Die Risikolimits sind dabei die Notbremse und werden von der **dritten und letzten line-of-defence** überwacht, der internen Revision. Siehe Details im Abschnitt 3.3 und Abschnitt 3.4.

$\Longleftrightarrow$ Die Risikotransparenz mit denen Mitarbeiter z.B. interne Informationen behandeln, wird maßgeblich von der Risikokultur und tone-of-the-top im Unternehmen beeinflusst.

$\Rightarrow$ Eine nötige Risikotransparenz soll auf alle Prozesse im Unternehmen wirken und kontinuierlich verbessert werden!

Alle oben angeführten Themen unterliegen keiner einmaligen Festlegung sondern einer regelmässigen Anpassung.

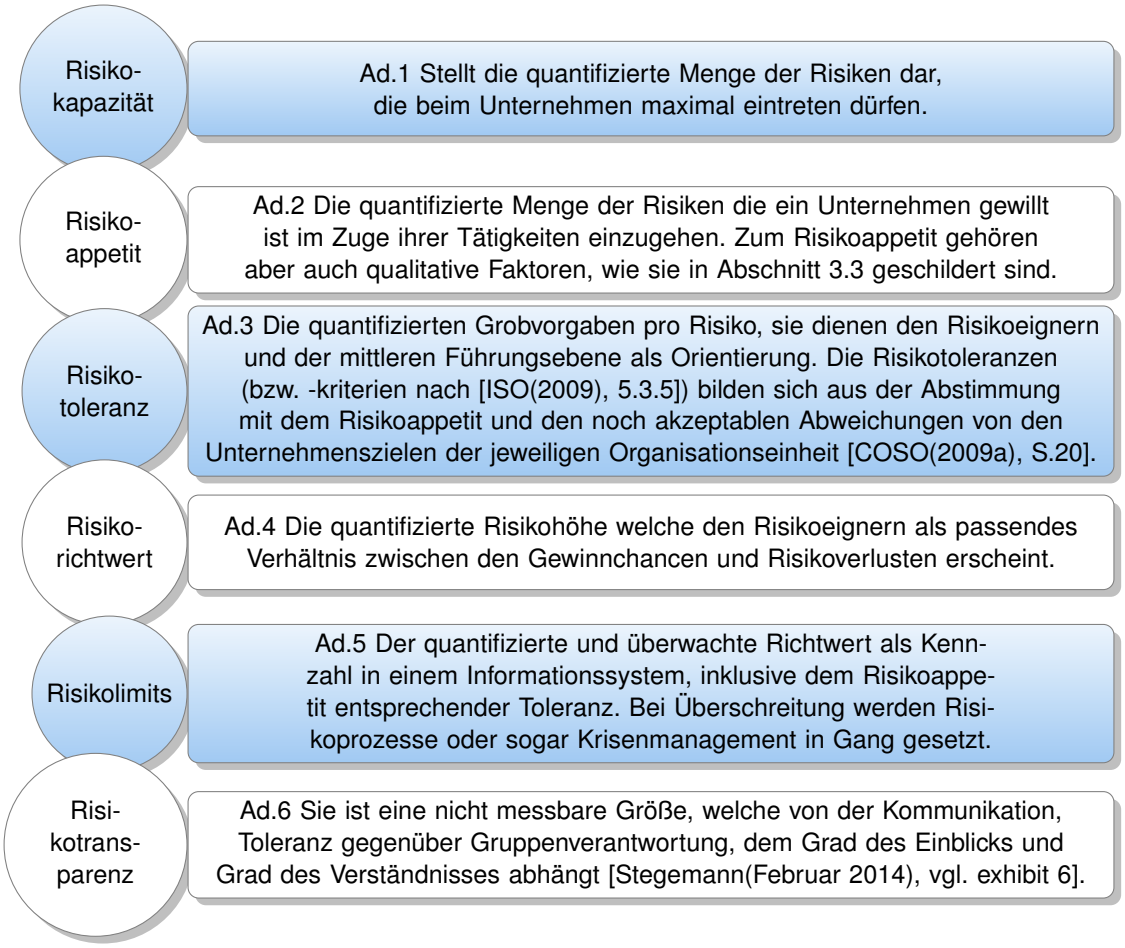


Abbildung 3.2: Zusammenfassung über die Unterschiede der in Abbildung 3.1 verwendeten Risikokennzahlen

Zielfindung

Die Zielfindung dient bei COSO als Schnittstelle zwischen dem Prozess und Rahmen. Die im Rahmen laut 3.3 beschriebene Verankerung des Risikomanagements innerhalb des Unternehmens basiert darauf, dass alle Risiken im Endeffekt auf Unternehmensziele wirken. Auf eben diese Ziele verweist daraufhin der komplette Risikoprozess, von Identifikation über Bewertung bis Steuerung, laut 3.5. Nach COSO werden die Ziele (engl. objectives) in Compliance-Ziele, Berichterstattung-Ziele (engl. Reporting), die strategischen Unternehmensziele und die daraus abgeleiteten operativen Ziele unterschieden [COSO(2009b), vgl. S.12-22]. Beispiele hierfür können sein:

- operative Ziele

  - Kostenkontrolle.
  - Optimierung des Cashflow.
  - Produktivitätssteigerung.
  - Qualitätsverbesserung.
  - Erhöhung der Kundenbindung durch Kundenzufriedenheit.
  - Einhaltung von Lieferzeiten.
  - Marketingstrategie erstellen.
- Ziele der Berichterstattung
  - Je nach Unternehmensform Einhaltung der Finanzberichterstattung.
  - Vollständige Dokumentation aller Geschäftsvorfälle.
  - Einhaltung aller Rechnungslegungsgrundsätze und Verpflichtungen in der Finanzbuchhaltung.
- Ziele der Regeleinhaltung (engl. Compliance)
  - Rechtliche Auflagen und Normen einhalten und somit Sanktionen wie Geldstrafen vermeiden.
  - Sicherheit am Arbeitsplatz und allen Geschäftsgebarungen.
  - Korruption vermeiden.
- Strategische Ziele
  - Marktführerschaft durch Kundenwachstum.
  - Oberstes Viertel der Produktverkäufe bei Wiederverkäufern sein.
  - Technologievorsprung.
  - Change Management.

Bei ISO werden durch das Erstellen des Zusammenhangs (sowohl während des Rahmens als auch Prozesses) die Ziele der Organisation zum Ausdruck gebracht. Es definiert die externen und internen Einflussfaktoren, die beim Risikomanagement zu berücksichtigen sind und legt den Geltungsbereich und die Risikokriterien für den nachfolgenden Prozess fest [ISO(2009), 5.3]. Im sogenannten Mandat wird festgelegt, dass die Ziele des Risikomanagements und die Risikoeinstellung (-appetit laut COSO) auf die Ziele und Strategien der Organisation abzustimmen sind. Des Weiteren ist sicherzustellen, dass die Organisationskultur und die Risikomanagementpolitik miteinander im Einklang stehen [ISO(2009), 4.2]. Beispiele für Ziele des Risikomanagements gehen von Existenzsicherung, Erhöhung des Unternehmenswertes, Senkung der Risikokosten bis zur Optimierung der Eigenkapitalausstattung [Romeike and Hager(2013), S.96].

Risiko Situation	1.Frage jeweils 1 bis 4	2.Frage (je 1-4)	3.Frage (je 1-4)	Score (9-36)
Wachstum	Leistungsdruck	Wachstumsrate	Unerfahrenheit der Topmitarbeiter	
Kultur	Belohnung für unternehmerische Risikonahme	C-Level-Resistenz gegenüber schlechten Nachrichten	Level des internen Wettbewerb	
Informationssystem	Geschäftskomplexität und -volatilität	Lücken in der Performance Diagnose	Ausmaß dezentraler Entscheidungsfindung	
Ergebnis				____
Erklärung	9-18: Sicherheitszone	19-28: Vorsichtszone	29-38: Dangerzone	

Tabelle 3.1: Risiko-Kalkulator nach [Simons(1999)]

Risikoappetit und -situation

Die Wahl des Risikoappetits nach Risikokategorien ist Entscheidung des Vorstandes. Die vorhandene Risikoeinstellung im Unternehmen kann von Risikoavers (vermeidend trotz höherem Grenznutzen), -neutral oder -liebend (bejahend trotz niedrigerem Grenznutzen) gehen [Stegemann(Februar 2014), vgl. S.11]. Ohne die Wahl des Risikoappetits, ist die Planung des Risikomanagement genauso wie die Konstruktion einer Brücke ohne die Flussbreite zu kennen [ERNST&YOUNGS(2010), S.I]. Der überwiegende Teil der Menschen sind risikoavers [Damodaran(2008), vgl S.27]. Es gibt viele Extrembeispiele aus der Technik, z.B. bei sicherheitskritischen Anwendungen in der Luftfahrt, in der eine Nullfehler-Toleranz vorherrscht und somit kein Risikoappetit zugelassen ist. Andere Privatwirtschaftliche Bereiche, wie jene der Startup-Finanzierung, lassen unbegrenzten Risikoappetit zu. Bei normalen Unternehmen obliegt es dem Vorstand. Dabei sollte die Frage nach den drei profitabelsten Risiken nicht vergessen werden [ERNST&YOUNGS(2010), S.2].

Für eine grobe Einschätzung der Risikosituation kann der folgende Risikokalkulator in Tabelle 3.1 nach [Simons(1999)] dienen. Dabei werden die 9 Fragen aus 3 Kategorien beantwortet, jeweils mit 1 für wenig zutreffen bis 4 für sehr zutreffend. Das Ergebnis spiegelt die Gesamtpunktezahl wieder. In der Sicherheitszone liegt die kritische Frage nahe: Geht das Unternehmen nicht zu wenig Risiken eingeht, um künftig erfolgreich zu sein? Auch Unternehmen in der Vorsichtszone, in der sich die meisten wiederfinden werden, sollten bei hohen Werten in 2 von 3 Kategorien ihre Risikosituation nicht unterschätzen. Denn solange man nur einen kritischen Risikobereich hat, kann man ihn noch gut überwachen (und gut schlafen), bei mehreren kritischen Risikobereichen wahrscheinlich nicht mehr! Bei Bewertung in der Dangerzone sollten die Alarmglocken läuten und Handlungen gesetzt werden, kurzfristig wären dies Kontrollsysteme und langfristig Risikomanagement.

Risikomanagementpolitik, -philosophie bzw. -leitsätze

Bei COSO fasst die Risikomanagementphilosophie die vorhandene Unternehmenskultur und -werte zusammen. Sie dient als Grundlage für die nächste Phase der Strategiefest-

legung und der Risikobehandlung im operationellen Tagesgeschäft [COSO(2009a), S. 19 und 27]. Auch ISO 31000 versteht unter Risikomanagementpolitik die Verknüpfung und Begründung der Ziele, die Gestaltung der Organisationsstruktur, Anpassung an die Unternehmenskultur und Beschäftigung mit den Verantwortlichkeiten [ISO(2009), 4.3.2].

Zusammenfassend stehen Risikomanagementpolitik, -philosophie bzw. -leitsätze für das Gleiche, es sind die Absichten und Ziele des Unternehmens betreffend dem Umgang mit Risiken. Sie werden von der Geschäftsführung in Form von verbindlichen Weisungen erlassen, langfristig ausgerichtet und sind laufend zu verbessern [Romeike and Hager(2013), S.96]. Schlussendlich steht man vor der Wahl, die eigenen Risikokonzepte als Philosophien bzw. Politik oder vereinfachte Risikoleitsätze zu formulieren. Die anwendungsnähere Lösung ist das Ersetzen der ausformulierten Risikomanagementphilosophie bzw. -politik durch einfachere Risikomanagement-Leitsätze, ähnlich dem praxisüblichen Unternehmensleitbild bzw. code-of-conduct [Denk(2008), S.268-270] und [COSO(2009b), vgl. S. 6-11].

Risikomanagementstrategie

Die Risikomanagementstrategie ist das Ergebnis aus Unternehmenszielen und Risikopolitik. Man kann auch sagen, dass die Risikomanagementpolitik und -ziele mit den Strategien verwirklicht werden [ISO(2009), 4.3.1]. Während der Strategiefestlegung müssen Risikoappetit und Unternehmensziele berücksichtigt werden und ob diese zu den finanziellen Möglichkeiten passen [COSO(2009a), S.28].

Die Anforderungen an die Risikostrategie können nach [MaRisk(2014), S.43] sein:

- Konsistenz der Geschäftsstrategie, ob die Risikostrategie in diese integriert ist und ob sie in detaillierte Teilstrategien unterteilt werden kann?
- Beinhalten die Ziele der Risikosteuerung die wesentlichen Kernaktivitäten und Maßnahmen um diese zu erreichen?
- Berücksichtigt die Risikosteuerung die wesentlichen Risikothemen, wie deren Aggregation, Toprisiken oder Konzentration? Sind Risikokennzahlen mit quantifizierten Risikoappetit und -toleranzen vorhanden und als Performancemanagement mit der Ertragssituation verbunden?
- Sind die passenden Risikomanagementstrukturen, -methoden, -märkte und -reifegrad beschrieben und begründet [Denk(2008), S.127]?

Eine erfolgreiche Einführung bedarf laut [Romeike and Hager(2013), S.94-97] eine gute Aggregation der Information, Kommunikation und die Lösung der Interessen- und Zielkonflikte der verschiedenen Zuständigkeiten. Auch globale Frühindikatoren können einen ersten Denkanstoß über die vorhandene Situation des Unternehmens geben und damit den Strategieprozess einleiten.

Auf das Strategiethema wird hier nicht eigens eingegangen, im Literaturverzeichnis können diverse Studien der Beratungsunternehmen herangezogen werden.

Risikokultur und Riskotransparenz

Die Risikokultur ist das Betriebsklima, in dem alle Angestellten und Führungskräfte einen bewussten Umgang mit Risiken und eine positive Fehlerkultur pflegen. Es muss integraler Bestandteil des Denkens und Handelns werden und somit ganzheitliches Verständnis in der Unternehmenskultur [Romeike and Hager(2013), S.162]. Wesentliche Werkzeuge damit die Risikokultur alle Mitarbeiter erreicht, sind Kommunikationsinstrumente, Schulungen, Richtlinien, Handbücher und im Idealfall der Einbezug der Risikoziele in die Leistungsbeurteilung [Denk(2008), S.265].

Nach ISO31000 gehört das Risikomanagement in die Arbeitskultur der Organisation eingebunden. Die Human- und Kulturfaktoren sollten berücksichtigt und dafür mit einem nötigen Mandat der Unternehmensführung ausgestattet werden [ISO(2009), 2.11, 3.h und 4.2]. Die Organisation hat, sowohl in deren Prozessen als auch im Rahmen, die Risikokultur kurz- und langfristig zu verbessern [ISO(2009), 4.2, 4.3.1, 4.6, 5.1 und 5.3]. Die Risikoeinstellung ist Teil der -kultur und steht für die Haltung der Organisation gegenüber der -steuerung [ISO(2009), 2.5]. Die Risikoeinstellung kann vereinfachend durch risikoavers, -liebend und -neutral beschrieben werden.

Nach COSO sind die Kultur und ethischen Werte eines Unternehmen im internen Umfeld zu analysieren und innerhalb von Risikomanagementphilosophie und -appetit zu formulieren [COSO(2009a), S.27-30].

Abbildung 3.3 zeigt eine Unterteilung der Risikokulturen nach McKinsey in vier Kategorien vgl. [Stegemann(Februar 2014), Exhibit 6].

- **Transparenz** - beginnt mit dem unternehmensweiten Verständnis der Strategie und bezieht eine geregelte Risikoverfolgung durchs ganze Unternehmen mit ein. Sowohl interne als auch externe Warnsignale werden intern kommuniziert. Das Führungsverhalten hat einen klaren Zugang zum Risikoappetit und klares Verständnis über die Risiken im Unternehmen.

- **Risikorespektanz** - Regeleinhaltung bei kritischer Hinterfragung der Bürokratie. Ähnlicher Risikoappetit zwischen Mitarbeitern und Organisationszielen zur Verhinderung von operativen Risiken und Korruption. Förderung von kooperativen über kompetitiven Verhalten, um ein Unternehmensklima mit gültigen Spielregeln zu schaffen, anstelle des “besiege das System Gedanken”. Besonders gilt das in Bezug auf die Vorzeigerolle der Führungskräfte.

- **Reaktionsfähigkeit im Risikoprozess** zur Förderung vom schnellen und proaktiven reagieren. Ähnlich einer Duo Dilligence sind faktenbasierte Entscheidungen gefragt. Dabei ist eine Unternehmenskultur mit einem Klima des Verantwortungsbewusstseins,der Innovationsfreudigkeit und des Anpassungswillen bei Marktveränderungen wichtig.

- **Kenntnisnahme der Risikosituation** - methodischer und hautnaher Zugang im gesamten Risikoprozess. Beginnend mit der tabulosen Identifikation bis zum ergebnisoffenen Diskurs während der Analyse und deren verantwortungsbewussten Lösungen

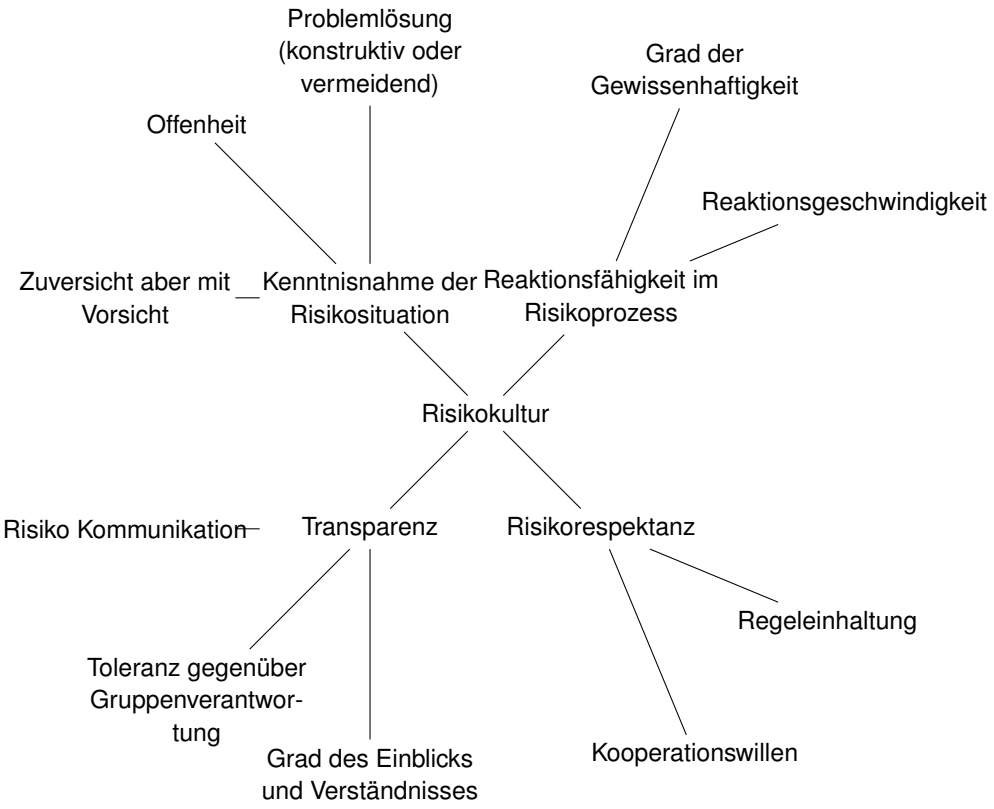


Abbildung 3.3: Elemente der Risikokultur [Levy(März 2015), Exhibit 1]

innerhalb der Risikosteuerung. Mitarbeiter sollen mitgestalten können, Grenzen respektieren und Meinungen hinterfragen dürfen. Ehrliche Berichte sollen belohnt werden und nicht die Angst vor schlechten Neuigkeiten.

Im industriellen Firmenumfeld nimmt die Wichtigkeit der Risikokultur und -appetit stetig zu [Pergler(Dezember 2012), S.7], [Power et al.(2013)Power, Ashby, and Palermo, Figure1]. Die London School of Economics hat eine Risikokultur-Studie in der britischen Finanzindustrie [Power et al.(2013)Power, Ashby, and Palermo, S.4-9] erarbeitet. Das kann auch für Industrieunternehmen als Anregung gelten:

- Laut Theorie sind für die Gestaltung der Risikokultur ethische Werte, Mitarbeitereinstellung aber auch Organisationskultur entscheidend. In der Praxis jedoch wird dies mit mäßigem Erfolg über Kennzahlen und Regeln in den Arbeits-, Informations-, Compliance- und Kontrollprozessen versucht. Dabei werden Kontrollen der 1. und 2. line-of-defence (kurz LOD) als überbürokratisch kritisiert und die 3. LOD mit interner Revision und Überwachung des Risikomanagement meist zu schwach ausgelegt. Ein kritischer Erfolgsfaktor ist der transparente und akzeptierte Organisationsaufbau zwi-

schen den LOD, insbesondere in Bezug auf Informationsflüsse und Entscheidungsfindungen.

- Es ist auf Überschneidungen und Doppelgleisigkeiten zu achten, beispielsweise komplett getrennte Management-Besprechungen mit Managementthemen und Risiko-Komitees mit Risikothemen. Die Verbindung und Balance von Risikoappetit mit den handelnden Risikoeignern und Management ist wichtig. Denn das Scheitern einer Risikokultur ist gleichbedeutend mit dem Zulassen von exzessiven und unkontrolliertem Risikoappetit, wie in der Finanzkrise 2007 erlebt. Passende Kennzahlen für die meist informelle Risikokultur zu finden, ist weiterhin eine offene Forschungsfrage, genauso wie einen passenden Dokumentationsprozess.
- Die Aggregation von Risikodaten ist auch bei der Risikokultur ein Qualitätsmerkmal, genauso wie die Eingliederung der Risikokultur in die Risikomanagement-Informationssysteme.
- Eine Möglichkeit ist es, Risikokultur und passende Risikomanager zu installieren und ihnen Zeit für eine kulturelle Akklimatisierung und evolutionäre Entwicklung zu geben. Denn Risikokulturen sind Prozesse:
  - die sich kontinuierlich und nicht statisch entwickeln
  - formale (organisatorische) und informelle (ethische) Bestandteile haben
  - heterogen in den Unternehmensbereichen und nicht einheitlich sind
- Respektvolles Sozialleben im Unternehmen nach [Power et al.(2013)Power, Ashby, and Palermo, S.21] kann am Beispiel Reporting erklärt werden:
  - durch Vertrauen z.B. in die Reports von anderen und deren reale Anwendung
  - durch die Ehrlichkeit in der offenen Wiedergabe der Beobachtungen, die zu Vertrauen führen
  - durch Selbstrespekt, also der Einbringung seiner eigenen Überzeugungen bei gleichzeitigem integrieren von anderen Meinungen
- Es gibt 4 Typen an Risikoexperten, die sich in der Art der Einflussnahme unterscheiden:
  - Compliance Champion, klärt die immer wichtigere Regulation.
  - C-Partner, beeinflusst durch persönliche Einflussnahme den Entscheidungsträger.
  - Technischer Champion, meistert die Komplexität und schafft einen einfachen Umgang, ähnlich einem Consultant.
  - Technischer Werkzeugmacher, schafft einfache und funktionale Risikomanagementmethoden und -werkzeuge.
- Dabei hat man in der Risikokultur nach [Power et al.(2013)Power, Ashby, and Palermo, S.32-35] sechs Zielkonflikte (engl. trade-offs) zu lösen :

1. Die Autoritätsrolle der 2. LOD-Risikoverantwortlichen, als Balance zwischen dem geschäftsnahen-partnerschaftlichen Umgang der 1. LOD oder der regulationsnahen Sichtweise eines Kontrolleurs der 3. LOD (engl. partnership-builders vs. overseers).
2. Die Organisatorische Eingliederung, als Balance zwischen formalen Hierarchien und informellen-interaktiven Netzwerken. Dies beinhaltet auch die Frage wann man besser top-down Methoden mit wenigen Involvierten oder bottom-up Methoden mit großen Gruppen benützt (engl. touch-point-enthusiasts vs. touch-point-realists).
3. Die Balance und Trennung von Risiko gegenüber Kontrolle, d.h. weder exzessive Überbürokratisierung, noch undisziplinierte Entscheidungen zu tolerieren. Dabei sind Transparenz und Geschäftsverständnis zur Ermittlung der Risikogrenzen nötig (engl. sandbox-guardians vs. gold-platers).
4. Der Beratungseinfluss im Unternehmen und dessen kritische Nutzung. Die Balance muss gefunden werden zwischen ständiger Nutzung von Beratern (d.h. ohne den Aufbau eigener Kompetenzen) und gefährlicher Intransparenz (d.h. ohne jede Nutzung von Beratungsdiensten) (enlg. sceptics vs. enthusiasts).
5. Der Regulierungsgrad und ab wann eine Über- bzw. Unterbürokratisierung vorherrscht. Darin fällt die Respektanz der öffentlichen Interessen, der Umgang mit Regulatoren ebenso wie die interne Meinung gegenüber Regulierung oder der Aufbau der eigenen 3. LOD (enlg. frictional vs. co-operative).
6. Der permanente Kulturwandel kann durch organisch implementierte Langzeitmethoden mittels “tone-from-the-top” oder ingenieurmäßigen Kurzzeitmethoden wie der Nullfehlertoleranz erfolgen. Auf jeden Fall muss das unter Bedacht der eigenen Unternehmenskultur und in den dringendsten Bereichen zuerst erfolgen (enlg. ethics and missions vs. disclinary).

Reifegrad des Risikomanagementsystems für Industrieunternehmen

Hier werden die Grundlagen für die praktische Umsetzung in Abschnitt 4.4 geschaffen.

Reifegradmodelle sind wichtig. Sie dienen zur Beurteilung des derzeitigen Reifegrades anhand von rechtlich-bindenden Richtlinien oder freiwilligen Benchmarks. Dabei sind unbedingt zwischen Aufgaben die wirklich notwendige regulatorische Mindestanforderungen sind und jenen empfohlenem Stand der Technik zu unterschieden. Reifegradmodelle werden zur Entscheidung der kommenden Verbesserungsschritte gebraucht.

Die Entscheidung über das angestrebte Reifegradziel des Risikomanagementsystems obliegt der Geschäftsführung und hat weitreichende Folgen, an Kosten und Zeitbedarf. Vorbildliche Unternehmen entwickeln ihr Risikomanagementsystem nicht als isolierte Prozesse [ERNST&YOUNGS(2010), S.1] und versuchen den Reifegrad des Risikomanagements an die Level der anderen Abteilungen, z.B. dem Projektmanagement, anzugleichen. Beispiele für Benchmarks findet man unter Abschnitt 4.9.

Es gibt sehr viele Reifegrad-Modelle. Fast jedes Fachbuch und Beratungsunternehmen hat leicht abweichende, eigene Vorstellungen, jedoch waren jene nach [Denk(2008), S.260-263] nicht zufriedenstellend detailliert. Dazu gibt es einen Mindestreifegrad, der gesetzlich vorgeschrieben ist, siehe Abschnitt 2.2.

Bei der Beurteilung von Reifegraden (maturity models) hat sich unabhängig vom Fachgebiet der CMMI Standard (Capability Maturity Model Integration) des Software Engineering Institute (SEI) der Carnegie-Mellon University etabliert. Dabei geben ursprünglich 5 Reifegrade die genau definierten Fähigkeiten bzw. Reife einer Organisation an, von Initial (Level 1), Repeatable (Level 2), Defined (Level 3), Managed (Level 4) bis Optimizing (Level 5) [1]. Dieses Model wurde adaptiert und auf 4 Level reduziert, um die so gern gewählte goldene Mitte in eine Tendenz Richtung besser oder schlechter umzuwandeln. Die Einteilung nach [Gleissner and Mott(2008), S.55-56] in 6 Level wird als übertrieben für Industrieunternehmen bewertet. Die Stufen gehen von 1. keinem Risikomanagement, 2. Schadensmanagement, 3. KonTraG-Risikomanagement, 4. ökonomisches Risikomanagement, 5. integriertes-wertorientiertes Risikomanagement und bis 6. holistisches Risikomanagement.

Die Reifegradlevel wurden mehrmals verändert, um die in der Praxis aufgetretenen Redundanzen zwischen Prozess und Verantwortlichen zu eliminieren. Des Weiteren wurden als Grundgerüst folgende Charakteristika zwischen den einzelnen Stufen nach CMMI Standard herangezogen.

1. Stufe spiegelt einen gesetzlichen Mindeststandard wieder, der fehlende Synergien aus dem Risikomanagement vermuten lässt.

2. Stufe zeugt von einer strukturierten Herangehensweise, sowohl in der Beurteilung als auch Bewältigung.

3. Stufe setzt quantitative, vollständige und normgerechte Umsetzung voraus. Das Risikomanagement wird auf allen Unternehmensebenen gelebt und verfügt über sinnvolle Prozesse, technische Methoden und IT-unterstützte Werkzeuge.

4. Stufe bedeutet, dass das Risikomanagement den aktuellen technischen Entwicklungsstand widerspiegelt und einem integrierten Ansatz verfolgt.

Die in dieser Arbeit gemachten, umfangreichen Recherchen werden anhand eines eigenen Reifegradmodells verarbeitet und bestehende unzureichende Modelle komplementiert. Aufbauend auf dem gängigen Standardmodell von CMMI, der ersten Adaptierung von Kultur, Prozess, Erfahrung und Anwendung nach [Hillson(1997)] und der Erweiterung mit den 3 lines-of-defense nach [Schleinzer(2014), Abb. 30]. Eine nicht verwendete Variante von einer Strategieberatung wurde in Abbildung 4.20 näher erklärt. Die aus Abbildung 3.1 enthaltenen Risikomanagement-Komponenten werden zur Beurteilung des Reifegrades herangezogen, siehe Abschnitt 4.4.

[1] `http://www.sei.cmu.edu/cmmi/`(25.09.2015)

3.4 Aufbau und Einbettung des Risikomanagements in die Organisationsstruktur

Die Organisationsstruktur wird ebenfalls im Risikomanagementrahmen der ISO 31000 [ISO(2009), Kp.4.2 und 4.3.4] und im internen Umfeld des COSO II Standard [COSO(2009a), S. 27ff] behandelt. Sie scheint hier als eigenes Unterkapitel auf, da sie eine zentrale Themenstellung bei der Anwendung im Unternehmen spielt.

Bei Aufbau und Einbettung des Risikomanagement in die Organisationsstruktur muss der Risikomanagementrahmen nach Abschnitt 3.3 durch die Unternehmensführung sichergestellt werden. Die Einbindung in bestehende Managementsysteme ist empfehlenswert, zur Erhöhung von Synergie und Benutzerfreundlichkeit. Bestehende Managementsysteme sind z.B. die Prozesse und Informationssysteme in der Strategieentwicklung, der Produktentwicklung, dem Qualitäts- oder dem Projektmanagement. Dabei ist eine individuelle Lösung zu entwickeln, die Unternehmensgröße, Führungskultur oder bestehende Risikopositionen der Branche stellen entscheidende Einflüsse auf die Gestaltung dar. [ONR(2014c), Kp. 4]. Die Fülle der Aufgaben benötigt eine Risikomanager-Position oder eine ganze Abteilung. Da viele kleine Unternehmen über keine ausdefinierten Managementsysteme verfügen, kann das Risikomanagement auch als eigenständiges Teilsystem konzipiert werden. Als Richtwert kann die Norm nach [ONR(2014c), Kp. 8] dienen.

Die Organisation für das Risikomanagement setzt folgende Begriffe und Definitionen voraus [Vanini(2012), S.263ff]:

- **Aufbauorganisation**, beantwortet wer Aufgaben erledigt und ist eine Zuordnung zum verantwortlichen Risikoeigner. Die aufbauorganisatorische Entscheidung im Unternehmen betrifft ob das Risikomanagement eine zentrale oder dezentrale Einheit werden soll. Ob diese eine eigene Stabstelle werden oder an eine bestehende Abteilung angehängt werden soll. Viele Industriebetriebe haben zwar eine ähnliche aber nicht einheitliche Organisationsform. Oft ist keine saubere Trennung zwischen ähnlichen Abteilungen gegeben. So werden Begriffe im Risikomanagement, interne Kontrolle, Controlling oder interne Revision oftmalig gemeinsam bzw. alternativ verwendet [RMA(2011), S. 13].

- **Ablauforganisation**, zeigt was erledigt gehört und ist somit eine sachliche, rechtliche, personelle und räumliche Regelung der Aufgabenerfüllung.

- **Institutionalisierung durch Integration oder Separation**. Die Integrationslösung steht für eine Übernahme von Aufgaben durch bestehende Stellen. Im Gegensatz dazu löst die Separationslösung die Aufgaben in einer eigenständigen Stelle.

    - **Integration** eignet sich für Unternehmen mit einem hohen Reifegrad in ihren Planungs-, Steuerungs- und Kontrollprozessen. Sie unterstütz hohe Risikobereitschaft der Unternehmensführung und bedarf einer guten Risikokultur und -bewusstsein der MitarbeiterInnen.

  - + Verbindet Sach- und Risikoentscheidungen.
  - + Bessere Risikoidentifikation durch die ebenfalls operativen handelnden Personen.
  - + Kostengünstiger durch Einsparung einer parallelen Organisationsstruktur.
  - − Fehlen eines institutionalisierten und unabhängigen Risikomanagements.
  - − Eventuelle Überlastung der Personen die sowohl das operative Geschäft als auch Risiken behandeln.
  - − Gefahr, dass Risikomanagement im Tagesgeschäft untergeht und somit mangelhaft ist.
- *o* **Separation** ist für spiegelverkehrte Unternehmen, jene mit niedrigem Reifegrad und Risikoaversion auf allen Ebenen.
  - + Hohe Priorität der Risikoaufgaben und Aufbau methodischer Kenntnisse.
  - + Entlastung der operativ tätigen Personen.
  - + Einheitliche Durchführung des Risikomanagements an allen Stellen.
  - − Fehlender Einblick in die Prozesse und Risiken der operativen Einheiten, dies bedarf dezentrale Risikostellen.
  - − Weniger spezifisches Fach- und Methodenwissen über das Risikomanagement der operativen Einheiten und schwache dezentrale Risikokompetenz.
  - − Gefahr von Doppelarbeiten und Koordinationsproblemen zwischen dezentralen Einheiten und dem Risikomanagement.

- Die Einordnung in die bestehende Unternehmenshierarchie kann durch Zentralisierung oder Dezentralisierung erfolgen, welches durch den Zentralisierungsgrad angegeben werden kann.
  - *o* **Zentrale Organisation des Risikomanagement** eignet sich bei geringer Umweltdynamik, Unternehmensgröße oder komplexer Struktur.
    - + Vermeidung von Doppelarbeit
    - + Übernahme der Koordination durch zentrale Stelle, bei gleichzeitigem Aufbau von Spezialwissen
    - + Einheitliche Durchführung des Risikomanagements auf allen Unternehmensebenen
    - − Verlängerung der Kommunikations- und Entscheidungswege
    - − Gefahr dass Wissen und Synergien in dezentralen Abteilungen nicht genutzt werden
  - *o* Unternehmen benötigen zu einem gewissen Grad ein **dezentrales Risikomanagement** wenn sie in einer dynamischen Marktumwelt tätig sind, große- oder komplexe Strukturen haben.
    - + Höhere Sachkompetenz für die Risikoidentifikation und -steuerung
    - + Mitarbeitermotivation ist durch Eigenständigkeit höher

  - + Fördert die Risikokultur
  - + Schnellere und flexiblere Prozesse und damit robusteres Unternehmen
  - − Gefahr von Doppelarbeiten
  - − Probleme bei bereichsübergreifenden Risiken
  - − Vernachlässigte Koordination schafft abweichende Prozesse und erschwert die Aggregation
- o **Mischform** etwa nach dem "dotted-line Prinzipöder als Matrixorganisation erscheint vor allem bei großen Unternehmen als nötig. Dabei bekommt das zentrale Risikomanagement als Verstärkung dezentrale Risikomanager in den Fachbereichen, die dies als Nebentätigkeit ausüben [Denk(2008), vgl. S.251].
  - + Allgemeine Vorteile von dezentralen Einheiten, Vor-Ort verbunden mit Vorteilen der zentralen Synergie
  - + Risikomanagement stellt keinen Fremdkörper da und kann durch bessere Einbindung schneller reagieren
  - − Typische Nachteile der Dezentralisierung wie etwa Doppelbelastung oder Konflikte bei Loyalitäten
  - − Gefahr der fehlenden Objektivität oder zu kollegialer Beziehungen, um kritisch handeln zu können
- o Eine aktuelle Organisationsform im Risikomanagement stellt das **three-lines-of-defense Modell** dar, dieses macht sich zusätzlich noch bestehende, artverwandte Abteilungen im Risikoprozess zu Nutze und wird im Abschnitt 3.4 erklärt.

Reale Organisationsstrutkuren im Risikomanagement

Die Unterscheidung zwischen den verwandten Abteilungen der Aufbauorganisation ist in Abbildung 4.1 dargestellt. Alle auf der Vorderseite erwähnten allgemeinen Merkmale von integrierten Abteilungen sind ebenfalls zu beachten. Eine erweiterte Erklärung der verschiedenen Abteilungen und Beurteilung der positiven und negativen Effekte bei Integration des Risikomanagement folgt anbei:

- Die **Interne Kontrolle** (kurz. IK bzw. meist IKS für ein IK-System) wird nach [Klinger and Klinger(2009), vgl. S.1-11] als Managementaufgabe erklärt. Innerhalb der 4 Aufgaben im Deming-Kreislauf von Planung, Umsetzung, Kontrolle und Erneuerung. IKS sind nicht einheitlich geregelt, bekannte Ansätze sind das amerikanische COSO I (1992) und deutsche KonTraG (1998). Kontrollaufgaben umfassen grob die Steigerung von Vermögenssicherung, betrieblicher Effizienz auf Prozesslevel, Zuverlässigkeit des Rechnungs- und Berichtswesen und Einhaltung von Vorschriften. Sie können auch in ein IKS mit seinen Hauptaufgaben Sicherheit, Wirtschaftlichkeit und Ordnungsmäßigkeit unterteilt werden. In kleinen Betrieben reicht für diese Kontrolle und Überwachung die Geschäftsführung aus, in größeren wird jedoch die Systematisierung der Kontrolle mit Prozessen und Methoden nötig. Details und Checklisten findet man bei [Klinger and Klinger(2009), vgl. S.61ff].

  - \+ Durch die Kontrolle der Prozesse unterstützt IKS automatisch das Risikomanagement [Gleissner(2011), S.235ff].
  - − Problematisch ist ein Schwerpunkt des Risikomanagement bei prozessorientierten Risiken und Kontrolltätigkeiten gegenüber Planung.

- Die **Interne Revision** prüft und hinterfragt kritisch die Prozesse im Unternehmen auf Effizienz und gesetzliche Einhaltung, z.B. ordnungsgemäße Geschäftsführung und Rechnungslegung. Die interne Revision verantwortet die Effizienzrisiken und überprüft als 3. line-of-defense (LOD) auch Risikomanagement und IKS (die 2. LOD) und das ganze Unternehmen (1.LOD) [Denk(2008), vgl. S.247].

- Mit **Externer Revision** sind die unabhängigen Wirtschaftsprüfer und deren Prüfung des Jahresabschlusses gemeint.

- Das **Controlling** dient mit Analysen und Informationen der Geschäftsführung bei ihrer Planung und Steuerung. Weiters beteiligt sich das Controlling bei der Gestaltung des Management-, Kontroll- und Risikoprozess, betrachtet Ziele ganzheitlich und ist das wirtschaftliche Gewissen [2]. Gängige Controlling-Methoden sind die Unternehmensplanung, Projekt- und Investitionsbewertung oder Balance Score Cards [Denk(2008), vgl. S.244].

  - \+ Controlling und Risikomanagement agieren oft mit der gleichen Datenbasis und haben besonders bei der Risikobewertung und Planung Überschneidungen.
  - \+ Erfahrungsaustausch und Erweiterung von Risikomanagement-Methoden wie Aggregation und Simulation sind auch für Controlling-Tätigkeiten relevant.
  - − Konzentration auf finanzielle Risiken resultieren eventuell in einer Vernachlässigung der nicht finanziellen Risiken.
  - – Bei Gleißner wird darauf verwiesen, dass neben dem normgerechten Risikomanagementansatz auch ein Controllingansatz generell möglich ist. Dabei werden Risiken immer als Planabweichung betrachtet und behandelt, dieser Ansatz wird in der folgenden Arbeit nicht verwendet [Gleissner(2011), S.243]. Generell ist der Begriff **Risiko-Controlling** sowohl im KonTraG, ONR49001 als auch in der Fachliteratur häufiger anzutreffen, nach der Dissertation von [Löhr(2010), S. 2ff] ist der Unterschied zwischen Risikomanagement und -controlling nicht eindeutig geklärt.
  - – Auch Gleißner zeigt als Variante ein zentrales Risikocontrolling mit Schnittstellen zu mehreren Abteilungen [Gleissner(2011), S.234ff].

- Die **Compliance** bedeutet übersetzt schlicht, ob das gesamte Unternehmen alle relevanten Gesetze und internen Vorschriften einhält. Dies zu überprüfen und einzuhalten liegt in der Verantwortung der Compliance [Gleissner(2011), S.238ff]. In der

[2] `http://www.igc-controlling.org/EN/_leitbild/leitbild.php`(24.2.2014)

Gesellschaft zeigt sich die, in den letzen Jahren stetig steigende, Bedeutung der Regulierung, Moral und HSE (engl. health, safety und environment). Für Unternehmer gibt es internationale Leitfäden, siehe [ICC(2013), vgl. S.61ff] und auch Spezialisten für die diversen Spezialthemen wie z.B. Korruption, Umweltschutz, Datenschutz und Wettbewerbsrecht.

  - − Gefahr besteht bei unvernünftiger Balance zwischen ökonomischen Entscheidungen und übertriebener Compliance, die insbesondere Einkauf, Verkauf oder Projektmanagement lahmlegen könnte [Gleissner(2011), S.234ff].

- o Weitere Details zum Compliance gibt die Studie nach [Reiß and Reker(2011)], deren Ergebnisse in Abschnitt 3.11 zusammengefasst werden.

- In großen Konzernen ist eine Aufteilung der Buchhaltung in Finanz-, Kreditoren- und Debitorenbuchhaltung üblich, dies sollte nicht mit der kompletten Finanzabteilung verwechselt werden. Bei der Integration des Risikomanagement in einen **Finanzbereich**, wie dem externen Rechnungswesen oder der Konzernfinanzierung, ist nach [Denk(2008), vgl. S.248-249] folgendes zu Bedenken:

  - + Risikomanagement erhält vollständige Informationen über kaufmännische Daten.
  - − Eine Konzentration auf rein finanzielle Aspekte und somit fehlende Neutralität oder Fachverständnisse gegenüber anderen Abteilungen.
  - − Im Vergleich zum eigenständigen Risikomanagement hat man sowohl eine geringere Nähe zur Geschäftsführung, als auch geringere Einbindung in die Prozesse.

- Weitere artverwandte Abteilungen sind etwa das **Qualitätsmanagement** . Je nach Branche können noch andere Abteilungen systemimmanente und natürliche Überlappungen zum Risikomanagement haben. Es ist eine legitime Herangehensweise des zentralen Risikomanagement auch spezielle Tätigkeiten an dafür geeignete Spezialisten abzutreten. Diese gehören als Schnittstelle definiert und gelegentlich abgestimmt [ONR(2014c), Kp. 4.2]. Beispiele hierfür sind: Datenschutz, spezielle Rechtsfragen, Lebensmittelsicherheit, Arbeitssicherheit, Gebäudezustand bzw. Facility-Management oder Korruptionsbekämpfung.

  - − Problematisch hier wär der jeweilige Abteilungsschwerpunkt und somit eher prozessorientierte Denkweisen und fehlendes Finanzverständnis.

- Das **Versicherungsmanagement** verwaltet, aus Sicht des Risikomanagements, Maßnahmen für einzelne Risiken. Sollte diese Abteilung überhaupt bestehen, sollte eine gemeinsame Koordination innerhalb des Maßnahmenplans und Projektmanagements erfolgen.

- Das **Notfall-, Krisen- und Kontinuitätsmanagement** beschäftigt sich mit bereits eskalierten Risiken bzw. erstellt Notfallpläne für Risiken mit Krisenpotential. Es ist somit

als Teil der Risikosteuerung miteinzubeziehen. Ein Risikomanagement das Notfall-, Krisen- und Kontinuitätsmanagement beinhaltet, nennt man auch umfassendes Risikomanagement [ONR(2014c), Kp. 4.2] .

- Vor- und Nachteile eines **zentralen Risikomanagement als alleinstehende Abteilung** gegenüber einer dezentralen Lösung:
  - \+ Die Nähe zur Geschäftsführung bringt mehrere Vorteile, wie Einbindung in Entscheidungsprozesse, gute Informiertheit und gesamte Unternehmenssicht.
  - \+ Die zentrale Risikomanagementabteilung handelt neutral gegenüber allen operativen Abteilungen und Themenstellungen. Sie spezialisiert sich auf Risikomanagementthemen.
  - \+ Da keine Mitarbeitergruppe alles nötige Wissen zum operativen Risikomanagement auf der untersten Unternehmensebene hat, empfiehlt [Kaplan and Mikes(06.2012), S.7] eine zentrale Risikomanagementgruppe zur Informationssammlung von den operativen Managern.
  - − Es sind klare Schnittstellen zu allen oben genannten Abteilungen nötig und in der Aufbauphase ist eine Isolation kritisch [Denk(2008), vgl. S.248].
  - − Eine eigene Stabstelle muss sich Durchsetzungskraft erst erarbeiten.

Ein Risikomanagementansatz (bzw. nach ISO Risikomanagementplan) skizziert das Vorgehen bei Aufbau und Organisation des Risikomanagementsystems und wird dabei wesentlich vom gesetzlichen Rahmen vorgegeben [Gleissner(2011), S.224ff]. Der nach Gleißner verwendete Begriff Risikomanagementansatz ersetzt bei ihm zum Teil den Risikomanagementrahmen, da Risikomanagementrahmen in seinem Konzept gar nicht erwähnt werden. Erneut ist bei den Begriffen Vorsicht geboten.

Ein eigenständiger Risikomanagementansatz steht zwar nicht dem Finanzsektor aber zumindest jedem Industrieunternehmen frei zur Auswahl. Es wird empfohlen ihn auf die Eigenheiten des eigenen Unternehmens anzupassen. Gängige Möglichkeiten sind dabei die zweistufige Organisation des Risikomanagements [Gleissner(2011), S.225]. Die mittels Risiko-Controlling-Stabstellen den Risikoprozess zwischen Management und Risikoeigner führt und bei jedem Tochterunternehmen gespiegelt und dezentral abläuft.

In einer Studie im Jahr 2011 von PWC (PricewaterhouseCoopers) und BDI (Bundesverband der Deutschen Industrie) wurden 1.021 mittelständische Unternehmen aus allen Branchen zur Organisation ihres Risikomanagements befragt. Nur ein Viertel waren mit ihrem Ist-Stand zufrieden [bdi and pwc(2011), Kp.3]. Ist-Stand laut Studie:

- Insgesamt haben 63% der Befragten eine spezielle und zentrale Risikomanagementabteilung. Unterschiede bestehen zwischen kleinen KMU (unter 100 MIO EUR) mit 54% und großen KMU (über 1.000 MIO EUR) mit 83% .
- Bei 73% ist das Risikomanagement im Controlling angesiedelt und 88% berücksichtigen Risiken in der Planung und Budgetierung.

- Nur 28% haben eine eigene Compliance-Abteilung.
- 68% haben zusätzlich Verantwortliche für einzelne, spezielle Risiken, bei Familienunternehmen sind es nur 60%.
- Nur 45% haben spezielle Risikomanagementgremien, Ausschüsse oder Komitees.
- Fast 90% aller Befragten beziehen ihre Tochtergesellschaften in das Risikomanagement mit ein.

Three-lines-of-defense als Modell für die Rollenverteilung eines mehrstufigen Risikomanagement im Unternehmen

Die Erklärung des Modells und praktische Umsetzung findet man im Risikomanagementhandbuch Abschnitt 4.4.

Wer das three-lines-of-defense Modell erfunden hat, kann weder in Fachbüchern noch wissenschaftlichen Publikationen nachgewiesen werden. Paradoxerweise ist es jedoch defacto Standard für Unternehmensführung (engl. Corporate Governance) in der Finanzbranche geworden [MaRisk(2014), S. 349], [Pergler(Dezember 2012), S. 7] und [Stegemann(Februar 2014), S. 12]. Somit ist es auch interessant für Industrieunternehmen.

In der Basel Committee Dokumentsuche reichen Erwähnungen des LOD-Modells bis ins Jahr 1999 zurück [3]. Auch in der britischen Finanzmarktaufsichtbehörde finden sich seit 2011 Referenzen auf LOD [FSA(2011), 1.11, 2.23, 2.24 und 3.9] [4]. Auch Beratungsunternehmen wie [Stegemann(Februar 2014), Exhibit 7] und KPMG [5] benutzen es ohne Erwähnung von Alternativen.

Die Abbildung 3.4 zeigt den in dieser Arbeit verwendeten three-lines-of-defense Ansatz, inklusive deren Zuteilung innerhalb der Organisationshierarchie, deren zu verantwortlichenden Risikokategorien. Die Risikokategorien liegen direkt in der eigenen Verantwortung wenn sie als Kästchen rechts daneben stehen und indirekt in Verantwortung als Kontrollinstanz wenn die darunter liegenden LoD diese verantwortet. Die groben Aufgaben sind [MaRisk(2014), vgl. S. 349ff]:

1. LoD: Einhaltung der zu beachteten internen Regelungen, internen Risikolimite und Gesetze bei der täglichen Arbeit.
2. LoD: Eine Kontrolle der 1.LoD mit einem ex-ante (im vor hinein), präventiven, prozessbegleitenden und beratenden Charakter. Aufbau der Risikomanagement Kompetenz und Struktur. Zusammenarbeit mit der Geschäftsleitung bezüglich preformancemanagement und Strategie.

[3] siehe [Basel(2011), §13, 14, 44 und 45] oder `http://www.bis.org/search/?category=--&lang=--&mp=all&sb=1&q=three+lines+of+defense&adv=&n=180` (29.09.2015)

[4] Die FSA wurde 2013 in FCA unbenannt, siehe `http://www.fca.org.uk/static/pubs/guidance/guidance11.pdf` (29.09.2015)

[5] `http://https://www.kpmg.com/RU/en/IssuesAndInsights/ArticlesPublications/Audit-Committee-Journal/Documents/The-three-lines-of-defence-en.pdf`

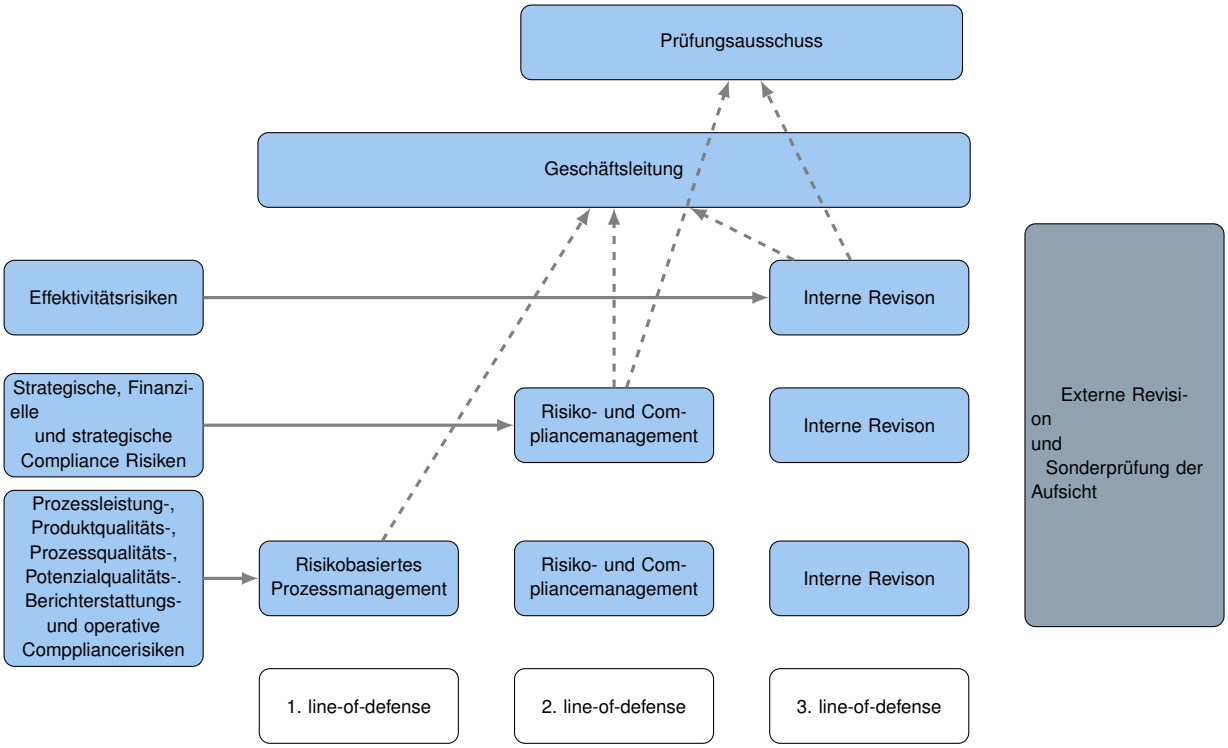


Abbildung 3.4: Three lines of Defense Modell inklusive zu verantwortende Risikokategorien, nach [MaRisk(2014), vgl. S. 349] und [Schleinzer(2014), vgl. Abb.22]

3. LoD: Eine Kontrolle aller LoD mit einem ex-post (im nach hinein) und auditiven Charakter. Überprüfung des Kontrollsystems

Der 2. und 3. LOD (insbesondere IKS, IR, Compliance, Risikomanagement) sind drei Besonderheiten gemein, die ihre Tätigkeit voraussetzt [MaRisk(2014), S. 349]:

- Uneingeschränkter Zugang zu allen Informationen, die sie für ihre Tätigkeiten brauchen. Wegen dem Auskunftsrecht des Vorsitzenden im Aufsichtsorgan dürfen sie diese Informationen an ihn weitergeben.

- Unabhängigkeit, dadurch hat die Geschäftsleitung einen verringerten Einfluss. Deshalb muss auf jeden Fall ein Wechsel der 2. und 3. LOD-Leitung dem Aufsichtsorgan mitgeteilt werden.

- Die Leiter dieser Abteilungen haben besonderen Qualifikationen und Anforderungen zu genügen, die zum Teil im gesetzlichen Rahmen vorgeschrieben sind.

Bei einer Studie im Jahr 2013 von KPMG und EIU (Economist Intelligence Unit) mit 1.092 teilnehmenden Unternehmen aus aller Welt, wurde das LOD Modell ebenfalls befragt [KPMG and EIU(2013), S.16-18] und folgende Einsichten erhalten:

- Entgegen der weit verbreiteten Meinung, sind 79% der Unternehmen mit der Effektivität des Risikomanagements in der 1. LOD mehr zufrieden, als mit 74% bei der 2. LOD oder 67% bei der 3. LOD. Besonders stark fallen unterschiedliche Bewertungen des LOD-Modells zwischen Unternehmen mit bottom-up-Risikomanagementprozess und jenen mit top-down-Risikomanagementprozess aus. Erstere bewerten die 1. LOD mit 86% bis 3. LOD mit 75% und letztere die 1. LOD mit 57% bis 3. LOD mit 32%. Daraus kann nur der Schluss gezogen werden, dass unternehmensweite bottom-up-Risikomanagementprozesse von Identifikation bis Beurteilung die beste Wahl darstellen. Sie fördern eine positive Risikokultur, transparente Kommunikation und schaffen effiziente Synergie bei den Risikoeignern.

- Die o.g. Bewertungen messen die Effektivität des gesamten Risikomanagementprozesses mit einer 4-stufigen Skala. Mehr als 20% haben sehr effektive Risikomanagementprozesse, rund die Hälfte ungefähr Gute, knapp 20% eher Ineffiziente und die restlichen 5 bis 10% sehr Ineffektive. Diese Ergebnisse zeigen Ähnlichkeit mit anderen Studien, wie [Stegemann(Februar 2014), Exhibit 4].

Weitere Modelle verweisen auf 5 oder 9 LOD, und zählen Versicherungsmanagement, Regulatoren, Krisenmanagement (engl. Resilience), Business Intelligence oder Security als line-of-defenses dazu [6]. Dies wird in dieser Arbeit als nicht sinnvoll betrachtet, insbesondere nicht für mittelständische Industrieunternehmen.

Einbettung des Risikomanagement über prozessorientierte Managementsysteme

Ein in dieser Arbeit nicht verfolgter Ansatz ist die prozessorientierte Implementierung des Risikomanagementsystems nach [ONR(2014c), Bild 3]. Dies wäre die Kopplung und Behandlung der Risiken innerhalb des Prozessmanagement und deren Software. Dabei handelt es sich um eine Einbettung des Risikomanagements in bestehende Systeme und damit verbundenen

- Wechselwirkungen mit Kernprozessen der Organisation, um die Prozess- mit den Risikoeignern zu verschmelzen [ONR(2014c), Kp. 3.1]

- Schnittstellen zu anderen Teilsystemen des Managements, inklusive deren IT-Umsetzungen.

Begründet wird das damit das integrierte Managementsysteme wie Prozess-, Arbeitssicherheits-, Umwelt-, oder Qualitätsmanagement bereits etablierte Ansätze und Methoden aus der

[6] `http://www.managementexchange.com/sites/default/files/media/posts/documents/corporate_oversight_and_stakeholder_lines_of_defense.pdf` (30.9.2015)

Praxis haben. Ein Integriertes Managementsystem nach ONR 49002-1 kann aus den Teilsystemen Qualitäts-, Umwelt-, Gesundheits-, Sicherheits-, Compliancemanagement, internes Kontrollsystem, Versicherungsmanagement, etc. bestehen. Über all diese Teilsysteme hätte das Risiko- und Krisenmanagement eine Querschnittsfunktion [ONR(2014c), Bild 7]. Gleißner benützt diesen Ansatz als eine Umsetzungsmöglichkeit, benennt diesen aber als Controllingansatz zur Umsetzung eines integrierten Risikomanagements [Gleissner(2011), S.226].

Diese Regelungsmöglichkeit ist im VDI 4060 Blatt 1 ebenfalls zusammengefasst und bietet eine Handlungsanleitung für integrierte Managementsysteme (kurz IMS). VDI 4060 Blatt 2 berichtet weiter über die diesbezüglichen Erfahrungen von 11 Unternehmen. Die Regelung sieht die Aufgabe darin potenzielle Unternehmensrisiken rechtzeitig in einem kontinuierlichen Verbesserungsprozess zu managen. Das ist ausdrücklich keine Einzelaufgabe. Bestenfalls wird eine Betrachtung aller Bereiche von Qualität, Umwelt und Sicherheit bis unternehmensspezifischen Sonderbereichen in einem einzigen integrierte Managementsysteme unterstützt. Im angelsächsischen Raum wird von HSEQ Systemen gesprochen (Health, Safety, Environment and Quality), wenn Anforderungen aus verschiedenen Bereichen z.B. Gesundheit, Sicherheit, Umwelt, Qualität in einer einheitlichen Struktur zusammengefasst werden [VDI(2005), S.1ff].

Gründe für ein prozessorientiertes integrierte Managementsysteme [VDI(2005), S.2]:

- Viele Standards werden auf freiwilliger Basis umgesetzt, um diverse spezielle Zertifizierungen zu erhalten, z.B. die DIN EN ISO 9001 für Qualitätsmanagementsysteme, DIN EN ISO 14001 für Umweltmanagement oder dem österreichische Corporate Governance Codex.

- Rechtliche Vorgaben z.B. in der deutschen Störfallverordnung, beim Arbeitsschutzmanagementsystem, einem Risikomanagementsystem ermöglichen bei einem integrierte Managementsysteme eine verbesserte Nutzung von Synergien.

- Wegen der verbesserten Übersicht über sämtliche Geschäftsprozesse und Schnittstellen zu externen Systemen ergibt sich eine Optimierung bei Kosten, Reaktionszeiten, Betriebsstörungen oder Unfallenverhinderung.

- Für Mitarbeiter ist die Nutzung eines einzigen Regelwerks und zentraler integrierte Managementsysteme verständlicher und motivierender.

- Durch integrierte Audits (dt. Überprüfungen), zentrale Verfolgung von Prüfungen und abgestimmte Maßnahmen werden Doppelgleisigkeiten vermieden.

- integrierte Managementsysteme haben eine erhöhte Rechtssicherheit, da man alle Geschäftsprozesse systematisch behandeln und mit den Soll-Anforderungen vergleichen kann.

- Prozessabläufe nehmen auf Einzelfragen wie Qualität, Umwelt und Sicherheit keine Rücksicht mehr. Die Prozesse führen die gesamten Anforderungen aus und werden als Ganzes (integriert) betrachtet.

Nicht zu verwechseln ist, dass ein integriertes Informationssystem ein Softwareprogramm bezeichnet, das Zugriff auf Daten aus verschiedenen Datenquellen ermöglicht (siehe Abschnitt 5.4) und so das integrierte Managementsystem unterstützt (siehe Abschnitt 5.1). Die Annahme in beiden Fällen ist, dass Benutzer beim Umgang mit Management- oder Datenaufgaben ein möglichst einfaches System wollen [Leser and Naumann(2007), S.7] und dafür ein hoher Grad an Transparenz gefragt ist. Die Ausgestaltung eines integriertes System, das mittels Metadaten verschiedene Datenquellen abbildet, sollte das Ziel jedes Unternehmen sein.

Weitere auf hier nicht eingegangene, prozessorientierte Modelle sind das Total-Quality-Management oder European Foundation for Quality Management (EFQM), die als internationale Richtlinien für Qualitätsmanagement mehrere Unternehmensbereiche integrieren, vgl. [Wagner and Patzak(2015), S.385ff].

Die Prozessmodellierung von Prof. Scheer mittels Y-Modell und dessen computerunterstützte Weiterentwicklung ARIS, ist eine Methode die den kompletten Entwicklungsprozess von der Modellierung des Geschäftsprozesses bis zum Anwendungssystem umfasst [Scheer(2013), S.5ff]. Derzeit existiert noch keine Standardsoftware, die den kompletten Betriebsprozess von Produktplanung, Vertrieb, Produktion, Qualitätssicherung, etc. beherrscht. Daher müssen Teilsysteme in Unternehmen eingesetzt werden. [Abts and Mülder(2013), S.69ff].

Einfluss zwischen Informationssystemen und Organisationsform

Meist haben Unternehmen über die Jahre eine Vielzahl an Informationssystemen im Einsatz, siehe Abschnitt 5.1. Dies erfordert eine Gestaltungsrichtlinie um folgende Vorteile in der Unternehmens-IT-Landschaft zu erreichen [Frick et al.(2009)Frick, Servaes, Abts, Mehrtens, Söhnchen, Mülder, Stegemerten, and Westheide, S.281ff]:

- Geschäftsprozesse qualitativ und quantitativ optimieren, wenn möglich unternehmensweit
- Investitionsschutz durch integrierte IT-Landschaft, z.B. durch Reduktion der Wartungskosten
- bei derselben Technologiegeneration zu bleiben reduziert aufwändige Wartungen und Tests
- Integration hat auch Nachteile, z.B. Kettenreaktionen bei Fehlern

Ob es eine ganze Anwendungs-Systemlandschaft gibt oder nur einzelne Informationssysteme übt im Unternehmen einen gegenseitigen Einfluss mit der Organisationsform aus. Sowohl durch die Managemententscheidungen als auch die tägliche Arbeit der Mitarbeiter

wird die Rolle der IT im Unternehmen geprägt. Eindeutige Aussagen über Vor- und Nachteile können nicht pauschal gefällt werden [Schwarzer and Krcmar(2014), S.81ff.].

Heutzutage organisiert die sogenannte Enterprise Architecture und deren Management die überlappenden Anforderungen zwischen IT und Geschäftsprozessen als eigener Unternehmensbereich [Schwarzer and Krcmar(2014), S.280ff.].

Die Gestaltung von Informationsmanagement-Prozessen und -Verantwortlichkeiten wird in der IT-Governance geregelt und von der IT-Compliance überwacht. Sie hängt wie beim Risikomanagement stark von Unternehmenskultur, -typ, -marktsituation oder -reifegrad ab. Weitere Entscheidungsbereiche sind [Schwarzer and Krcmar(2014), S.278ff.]:

- IT-Architektur
- IT-Prinzipien
- IT-Applikationen
- IT-Infrastruktur
- IT-Investitionen und deren Priorität

Verantwortlichkeiten und Rollenbilder innerhalb des Risikomanagements

Die Frage nach der Gestaltung des Risikomanagements führt schnell zur Kernfrage, wie man das nun personell in der Organisation gestalten soll. Eine praktische Umsetzung findet sich im Abschnitt 4.4.

Weitere zahlreiche Beispiele für Stellenbeschreibungen findet man sowohl in der Fachliteratur wie [Gleissner(2011), S.246ff], [Denk(2008), Kp. 5.3] oder [Romeike and Hager(2013), Kp. 3.4], als auch in den Gesetzestexten Abschnitt 2.2.

Generell soll das Risikomanagement nicht direkt die Risiken managen. Diese Verantwortung liegt bei den operativen Risikoeignern und der Unternehmensleitung. Somit ist die Rolle des Risikomanagements ein effektives Risikomanagement zu schaffen, durch passende Risikokultur, -infrastruktur, -methoden, -werkzeuge und vor allem Transparenz [OpRisk-Advisory and Towers-Perrin(2010), S.36].

Der Aufbau eines mittelständischen Risikomanagements ist nach der Auffassung dieser Arbeit durchaus eine Vollzeitbeschäftigung. Die Führung eines etablierten Risikomanagements erscheint genauso als Vollzeitbeschäftigung oder zumindest gekoppelt mit einem artverwandten Bereich.

3.5 Grundlagen des Risikomanagementprozesses

Die Schritte des Risikomanagementprozesses sind in der ISO 31000 klar beschrieben und unterteilt. Die Äquivalenz diesbezüglich wird in Tabelle 2.2 und [COSO(2009a), S.27ff] beschrieben und sind die COSO II Komponenten 3 bis 6:

1. **Internes Umfeld**, beschreibt Bestandteile des Risikomanagementrahmen, siehe Abschnitt 3.3 .
2. **Zielfestlegung**, beschreibt Bestandteile des Risikomanagementrahmen, siehe Abschnitt 3.3.
3. **Ereignisidentifikation** wie in ISO 31000. Siehe Abschnitt 3.6.
4. **Risikobewertung**, wird in ISO 31000 Risikobeurteilung genannt und ist dort unterteilt in Analyse und Bewertung. Siehe Abschnitt 3.7.
5. **Risikosteuerung**, wie in ISO 31000. Siehe Abschnitt 3.8.
6. **Kontrollaktivität**, hier bestehen keine sauber trennbaren Unterschiede zwischen COSO und ISO, wobei die Grundidee der Kontrolle gleich ist. Im Sinne eines Regelkreises garantiert die Kontrolle die ständige Verbesserung des Risikomanagementsystems und stellt sicher dass Maßnahmen umgesetzt werden. Siehe Abschnitt 3.9.
7. **Information und Kommunikation** als Grundlage der Zusammenarbeit in einem Unternehmen. Siehe Abschnitt 3.10 und Kapitel 5 .
8. **Überwachung**, beschreibt eine unabhängige Instanz im Unternehmen, die die Effizienz und Ordnungsmässigkeit des Risikomanagementsystems überprüft. Sie betrifft Risikomanagementrahmen und -prozess. Siehe Abschnitt 3.11.

Der ISO 31000 Risikomanagementprozess folgt zwei Deming-Regelkreisen wie in Abschnitt 2.2 geschildert und entstand aus vielen Vorgängernormen. Interessante Vorlagen sind die Flussdiagramme der kanadischen Q850 oder australischen AS/NZS 4360 Risikomanagementnorm und der DIN IEC 62198 Projektmanagementnorm, wie in Abschnitt 2.6 geschildert.

Die Abbildung 3.5 zeigt den in dieser Arbeit verwendeten Ansatz nach [DIN and IEC(2001), Bild 5] und [ISO(2009), Bild 1].

Natürlich gibt es noch weitere Varianten von Risikomanagementprozessen, die zum Teil Rahmen mit Prozess vermischen wie beim pwc-Risikomanagementkreislauf [pwc(2011), Abb. 5] oder Abschnitt 4.9.

Methodenübersicht für den Risikomanagementprozess

Es gibt für jeden einzelnen Prozessschritt eine Unzahl an akzeptablen Methoden, wie in Abschnitt 4.3, Tabelle 3.2 und im ganzen Kapitel aufgezeigt. Eine detaillierte Erklärung jedes einzelnen Prozessschrittes und dessen Methoden erfolgt in den anschließenden Unterkapiteln.

Die Methoden müssen für den effizienten Einsatz zum Unternehmen passen! Die Bewertungssymbole stehen für Methoden die $+$ geeignet, $++$ gut geeignet und $+++$ sehr gut geeignet sind:

Die einzelnen Methoden aus Tabelle 3.2 werden in den Unterkapiteln im Detail erläutert. Auch [Romeike and Hager(2013), vgl. XV-XVI] bewertet einige Risikomethoden, auf diese

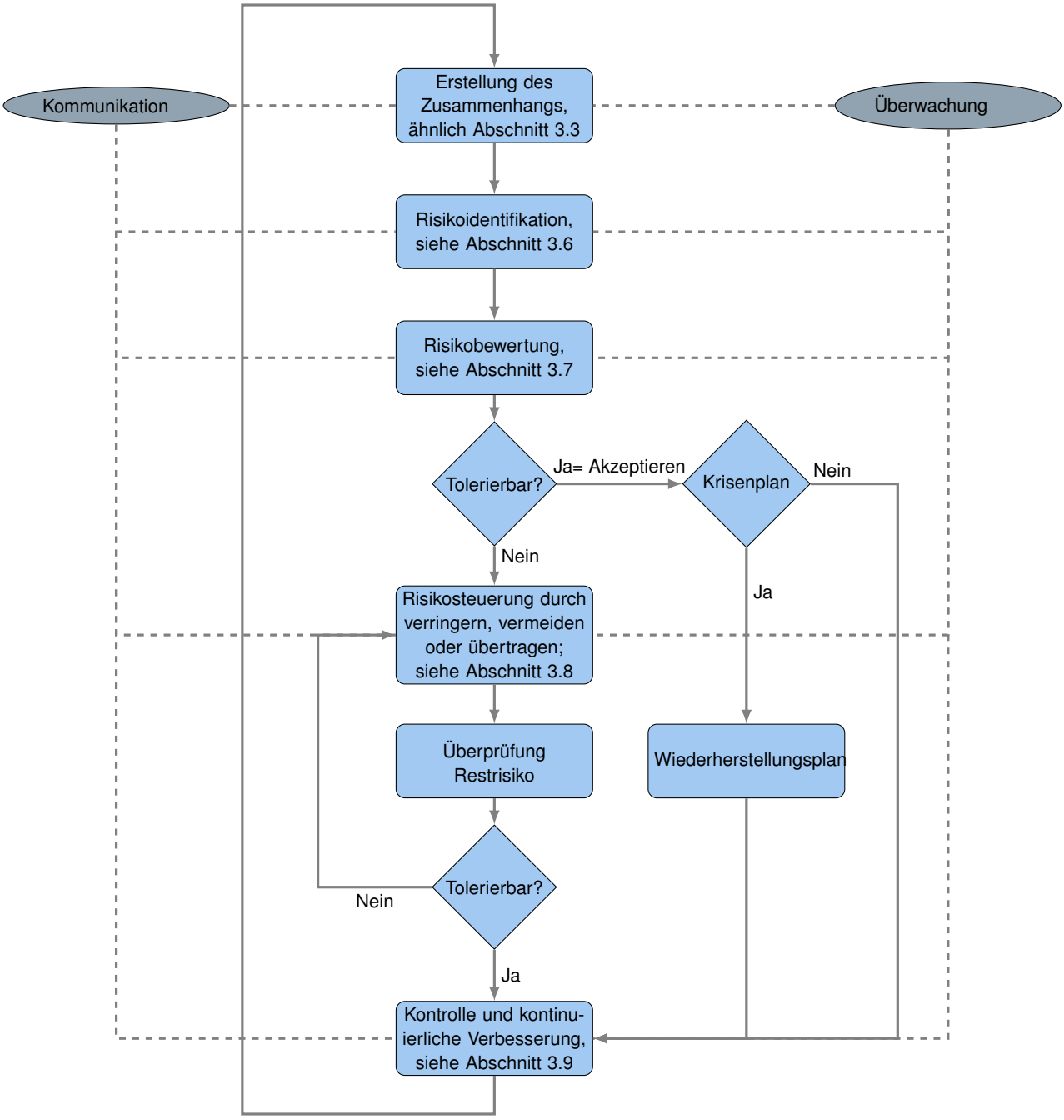


Abbildung 3.5: Risikomanagement Prozess nach [DIN and IEC(2001), Bild 5] und [ISO(2009), Bild 1]

Methode	Identifikation	Bewertung Bedeutung	Bewertung Häufigkeit	Bewertung Risikohöhe	Bewältigung
Brainstorming	+++	+	+		+
Delphi-Technik	++	++	++		++
World Cafe	+++	+	+		
Bürgerkonferenz	+++	++	+		+
Schadensanalyse	++	+	+		+++
London-Protokoll	+++	+			+++
Fehlerbaum- und Ablaufanalyse		++	+++	+	+
Szenerio-Analyse	+++	+++	++	++	+++
Critical Incident Reporting System	+++		+		++
Change Based RM	+++	+		++	
FMEA (Failure Mode and Effects Analysis)	+++	++	++	+	+++
Gefährdungsanalyse	++	+++	++	++	+++
HAZOP (Hazard and Operability Study)	+++	+++	++	+	+++
HACCP (Hazard and Critical Point)	++	++			+++
Standardabweichung		++	+++	++	
Konfidenzintervall		++	+++	++	
Monte-Carlo Simulation	+	++	+++	++	

Tabelle 3.2: Methodenübersicht für den Risikomanagementprozess nach ONR49002-2 [ONR(2014d), Tabelle 1]

wird in dieser Arbeit jedoch nicht mehr näher eingegangen. Eine Auswahl der für KMU passenden und erprobten Methoden sind in Abschnitt 4.5 aufgelistet.

3.6 Risikoidentifikation

Zusammenfassung der Risikoidentifikation:

$Das\ ist$ Die Risikoerkennung orientiert sich sich an den Zielen der Organisation, versucht gewissenhaft Risiken und Chancen, und Hintergrundinformationen zu dokumentieren [ISO(2009), vgl. S.26]. Die Risikoklassifikation ist der Abschluss der Risikoidentifikation, in dem Risiken mit einer gleichen Charakteristik gruppiert und Duplikate gefiltert werden. Ohne Kategorien können die weiteren Schritte des Risikomanagementprozesses kaum behandelt werden, genauso wie die Qualität des gesamten RM auf der Leistung während der Identifikation aufbauen [Denk(2008), vgl. S.84-85] .

$Grundlage$ Das Unternehmen hat einen passenden Risikomanagementrahmen inklusive Risikotransparenz, Risikokultur und tone-of-the-top, siehe Abschnitt 3.3.

$Kriterium\ 1$ Ein Konzept der Herangehensweise muss erstellt werden, dies beinhaltet, in Absprache mit der Unternehmensführung, die Ziele des RM, Auswahl von bottom-up oder top-down Methoden, Dokumentvorlagen und involvierte Personen [Denk(2008), vgl. S.84-85] .

$Kriterium\ 2$ Die Auswahl einer oder mehrerer Identifikationsmethoden die zum Unternehmen passen.

$Kriterium\ 3$ Elemente einer Risikoidentifikation sind jene die man in eine Dokumentation oder Datenbank einträgt. Es sind nach [Denk(2008), vgl. S.90] eindeutige Kennung, Risikomelder, Risikobezeichnung, Beschreibung, Kategorie, Vermerke, Quellen, Einflussgrößen, Indikatoren, erste Schätzungen, Maßnahmenideen, etc.

$Kriterium\ 4$ Erstellung von Risikokategorien die zum Unternehmen passen.

$Ziel$ Die Risikoidentifikation sucht zielgerichtet, rechtzeitig, regelmässig, schnell, vollständig, wirtschaftlich, systematisch und prozessorientiert nach Risiken und Chancen und erfasst diese in für die weitere Verarbeitung passende Form [Denk(2008), vgl. S.82-83] .

$Nachfolge$ Das Verstehen von Risiken und deren Bewertung, siehe Kapitel Abschnitt 3.7.

Innerhalb einer Organisation tragen viele Bereiche spezifische Risiken und haben bereits etablierte Bewertungs-, Planungs-, oder Kontrollmethoden. Die daraus erhaltenen Ergebnisse sind einerseits in ein RM zu integrieren und andererseits ist darauf zu achten eine einheitliche Vorgangsweise zu erhalten. Diese einheitlichen Vorgaben seitens des Risikomanagement schaffen vergleichbare Bewertungsskalen und aggregierbare Risiken in konsistenten und redundanzfreien Risikokategorien [pwc(2008), vgl. S. 34].

Weiters sollten andere Abteilungen im Unternehmen etablierte Risikobeurteilungen haben (engl. risk assessment), bietet sich eine Zusammenarbeit mit dem Risikomanagement an. Klassische Beispiele sind Strategische-, Operative (engl. operational)-, Compliance-, Interne Audit-, Finanzberichterstattung (engl. financial statement)-, Betrug- (engl. fraud) -, Marktrisiko-, Kreditrisiko-, Kunden-, Lieferanten-, Produkt-, Security-, IT- oder Projekt Risikobeurteilungen.

Ansätze zur Risikoidentifikation

Die generelle Herangehensweise ist bei der Identifikation die erste nötige Entscheidung. Die Identifikation kann durch die progressive Methode (engl. bottom-up method), wie Expertenworkshops oder Brainstorming erfolgen, d.h. an den Risikoquellen direkt in allen Unternehmensebenen. Die retrograde Methode (engl. top-down method), wie Beratungsprojekte oder in Kombination mit Planungs- oder Performancemanagement, analysiert mit der Unternehmensführung welche Risiken die Ziele und Strategien des Unternehmens beinhalten, siehe [Denk(2008), S.84-87] oder [Diederichs(2012), S.53ff]:

- Der Bottom-up Ansatz im Detail [Denk(2008), vgl. S.84-86] und [KPMG and EIU(2013), S.16-18]:
  - + Nutzt alltägliche Erfahrungswerte aller Mitarbeiter, dies beinhaltet ebenfalls Lösungsideen, Verbesserungen und Chancen!
  - + Schaffung eines Risikobewusstseins und Verbesserung der Risikokultur
  - − Übertriebene Granularität führt zu großen Risikolisten (Risikoinventaren), die dann in einen zweiten Schritt aussortiert und in Kategorien sortiert werden müssen.
  - − Hohe Kosten, durch Einbindung aller Unternehmensebenen und Einschulung vieler Mitarbeiter.
  - − Fehlendes Gesamtbild.
- Der top-down Ansatz im Detail [Denk(2008), vgl. S.84-86], [McNish(März 2013), vgl. S.12] und [Brodeur(August 2010)]:
  - + Effiziente und kostengünstige Methode, die den Blick und die Ressourcen auf die Toprisiken fokussiert. Sie ist für kleine Unternehmen gut geeignet, mit stark involvierter Geschäftsführung.
  - − Übersehen von Risiken und Chancen, für die Geschäftsführung keine neuen Sichtweisen.
  - − Keine detaillierte Analyse möglich, wegen fehlendem Detailwissen und Einblick in die spezifische Unternehmensrealität.
  - − Risikoeigner und Mitarbeiter arbeiten unverändert weiter, dabei besticht gerade der Risikomanagementprozess durch seine Einbindung in die Geschäftsprozesse.

  - Mitarbeiter müssen durch separate und abstraktere Workshops ins RM eingearbeitet werden.

- Eine Verknüpfung der beiden Ansätze kann laut [Denk(2008), vgl. S.86] bedeuten, repräsentativ ausgewählte Mitarbeiter aller Bereiche mit der Geschäftsführung zusammen zu bringen. Im ersten Schritt arbeiten sie einen Risikokatalog aus, im zweiten Schritt wird dieser dann unternehmensweit befüllt und bewertet. Dabei dient der zentral ausgearbeitete Risikokatalog als Orientierungshilfe für die dezentrale Identifikation. Abschließend werden dann Mehrfachnennungen, Aggregationen, Abhängigkeiten, Chancen, Ideen, etc. vom zentralen RM aufgearbeitet.

Nach [Diederichs(2012), S.86-87] gibt es auch natürliche Grenzen der Risikoidentifikation. Diese Grenzen beginnen mit der Wirtschaftlichkeit die eine vollständige Identifizierung verhindert und ziehen sich den ganzen Risikoprozess durch die die hohe Komplexität großer Unternehmen bei Ganzheitlichkeit, Interdependenzen oder Informationsfülle. Schließlich ist auch die Risikokultur die es bei allen MitarbeiterInnen durchzusetzen gilt schwer zu erreichen. Dabei ist aber zu beachten, dass Risiken selbst bei Unklarheiten, wie unbekannter Ursache oder Quelle, trotzdem ins Risikoinventar aufgenommen werden müssen, [ISO(2009), vgl. S. 26]! Der eigentliche Beginn liegt bereits in der Natur des Risikos mit einer eingeschränkten Objektivität, denn Einschätzungen hängen immer vom Standpunkt des Betrachters ab. Unternehmen die dem Risikomanagement einen evolutionären Prozess mit der nötigen Zeit und regelmäßigen Wiederholungen ermöglichen, werden aber daran nicht scheitern sondern wachsen.

Methoden zur Risikoidentifikation

Methoden zur **Risikoidentifikation** , wie in der Übersicht Tabelle 3.2 aufgelistet, sind beispielhaft und können oft kombiniert werden. Es muss auf die Situation im Unternehmen eingegangen werden. Bestenfalls ist die Risikoidentifikation in die bestehenden und periodisch durchgeführten Prozesse zu integrieren! Weiters ist auf die Details der jeweiligen Methode einzugehen:

- **Experten- und Mitarbeiterbefragungen** dienen zur Ermittlung der bereits irgendwo im Unternehmen bekannten Informationen. Eine weitere ähnliche Möglichkeit ist das Brainstorming. Dabei ist wichtig, “übe keine Kritik; je mehr Ideen, desto besser; ergänze und verbessere bestehende Ideen und je ungewöhnlicher die Idee, desto besser!” [Romeike and Hager(2013), S.110]. Bei all diesen Varianten ist besonderes Augenmerk auf die Zusammensetzung der Gruppe zu legen. Die Ergebnisse müssen in jedem Fall bereinigt und strukturiert werden [Denk(2008), S.90-91] . Denk warnt ausdrücklich davor, den in der Praxis weit verbreiteten Ansatz zur schriftlichen Umfrage zu unterlassen. Eine systematische Zusammenfassung von vielen ähnlichen und mässig formulierten Risiken sei schwer möglich und gerade der unternehmensweite und persönliche Risikomanagementprozess sei wichtig [Denk(2008), vgl. S.87] .

Risiken und Chancen sind zwei Seiten einer Medaille. Während der Expertengespräche werden beide Seiten besprochen und erfasst. Verbesserungsvorschläge können explizit aufgelistet werden.

- **Workshops** nach [Denk(2008), S.91-92] können einzeln oder unternehmensweit für die Ermittlung der Risiken durchgeführt werden und auch periodisch wiederkehren. Beispielhaft für die Ergebnisse eines Workshops sind Abbildung 3.6 und Abbildung 3.8.

  - Der Vorbereitungsaufwand ist nicht zu unterschätzen, denn die richtigen Mitarbeiter müssen alle gleichzeitig anwesend sein. Es bedarf einer Moderation, die auch fachliche Kenntnisse mitbringt und ständig das sensible Diskussionsklima zwischen höflich, ehrlich, unemotional und zielführend wahren muss.
  - Die Einschränkung auf Kleingruppen mit einstelliger Teilnehmerzahl machen oft unternehmensweit multiple Workshops nötig. Vorteil ist die gesteigerte Produktivität durch z.B. spezialisierte Themenblöcke.
  - Zu Beginn können Eisbrecher-Spiele, Vorstellungsrunden oder Brainstorming die Atmosphäre lockern und zugleich produktiv in die Materie einleiten.
  - Das Risikomanagement muss vorgestellt werden, deren Ziele, Wichtigkeit und der heutige Tag im Kontext zur Gesamtplanung sinnvoll erscheinen. Die konkreten Methoden, Systemelemente und Aufbau ebenso.
  - Auch Chancen und Verbesserungsvorschläge müssen kommuniziert und dokumentiert werden.
  - Die Hauptaufgabe der Workshops ist die Erstellung, Bearbeitung bzw. Systematisierung des Risikokatalogs und die detaillierte Besprechung aller nur erdenklichen Risiken. Hier fällt auch die Meinungsbildung darunter. Oft werden das Verständnis und die Einschätzung über einzelne Risiken zwischen den verschiedenen Teilnehmern auseinandergehen.
  - Natürlich liegt eine anschließende Risikobewertung nahe, sie hängt vom Stadium des RM ab. Handelt es sich um eine Einführung, ist aufgrund der Zeitlimitierung und nur oberflächlichen Kenntnis des RM, maximal eine erstmalige (schnelle) Schätzung zur Priorisierung nützlich. Handelt es sich um einen Workshop der bereits mehrere Jahre erfolgreich wiederholt wurde, dann ist die aktualisierende Risikobewertung sowieso der Hauptgrund dieses Workshops.
  - Workshops müssen wie jede andere Methode schriftlich dokumentiert werden. Dafür kann bereits eine Softwarelösung dienen, es muss keine spezialisierte Software für Risikomanagement sein. Business-Prozess- oder Planungssoftware kann je nach bestehen im Unternehmen ebenfalls erweitert werden.
  - Die Frage ob Führungskräfte bei einem Workshop teilnehmen, ist offensichtlich eine zweischneidige Sache. Das positive Commitment (tone-of-the-top) steht dem Eindruck der Kontrolle gegenüber. Einige Mitarbeiter können in Anwesenheit ihrer Vorgesetzten auch nicht offen reden.

  - Ein derart strukturierter Workshop schafft besonders bei der Einführung die Etablierung eines unternehmensweiten Risikomanagementsystem und -kultur im laufenden Betrieb.

- **Betriebsbesichtigungen** können vor allem bei Fertigung oder operativen Abteilungen Aufschlüsse bringen [Denk(2008), S.94] .

- **Risikochecklisten** als standardisierte Fragebögen, die eine systematische Erfassung erlauben, sind in der Praxis eine sehr unkomplizierte und damit beliebte Methode [Denk(2008), S.95]. Die Gefahr einer nur formal am Papier erfolgten Erfüllung der Compliance ist immer gegeben.

- Die **Zerlegung der Wertkette des Unternehmens** nach [Diederichs(2012), S.59] orientiert sich an der im Wirtschaftsingenieurwesen beliebten Wertstromanalyse (engl. value-stream-analysis). Diese Methode des Lean Management ist ein Modell zur Darstellung der Material- und Informationsflüsse einzelner Prozesse. Prozess ist hier gleich bedeutend mit dem Wertstrom den dieser erzeugen soll. Dies liefert somit eine Detailanalyse die nur bei besonders risikobehafteten Bereichen nötig wird, [Becker(2005), S.139-145]. Dieses Vorgehen ist wie im beispielhaften Aufbau eines Unternehmens in Bereichen dargestellt, siehe Abbildung 3.7. Jeder Bereich hat mehrere Prozesse und diese sind in mehreren Prozessschritten aufgezeichnet, die sich zur Ermittlung von Risiken und Chancen gut eignen. Zusätzlicher Vorteil ist dass darauf folgend eine Optimierung möglich ist. Nachteil dieser Methode ist ihre mangelnde Tauglichkeit zur IT Datenverarbeitung [Becker(2005), S.160].

- Mit Hilfe **der Prozesskettenanalyse** wird systematisch eine Analyse der operativen Geschäftsprozesse vollzogen, unter Einbezug der Prozessverantwortlichen, nach [Diederichs(2012), S.62-69] und [Becker(2005), Kp. 6]. Diese Methode ist gut geeignet für Unternehmen, die ihre Prozesse bereits in Flussdiagramme abgebildet haben oder durch diese Art der Risikoidentifikation einen mehrfachen Nutzen erzielen wollen. Bei der Modellierung des Prozesses werden überall die 7 W-Fragen nach dem was, warum, wer, wie, wann, wo und wie viel gestellt und dann als Flussdiagramme (sogenannte Prozessbäume) schrittweise abgebildet, inklusive einem Symbol für etwaige Risiken. Anschließend können alle Risiken in einer Risiko-Kontroll-Matrix wie in Tabelle 3.3 gezeigt, verwaltet werden.

- Die **Netzwerktechnik** ermöglicht eine Simulation von strategischen Entscheidungen mittels Systemtheorie und ist somit eine Verknüpfung vieler einzelner Einflussfaktoren zu einem Gesamtbild. Das gibt Aufschluss auf künftige Risiken [Diederichs(2012), S.59].

- Auch **Frühaufklärungssysteme** können der Risikoidentifikation dienen, durch frühe und systematische Beobachtung externer und interner Risikoquellen verbleibt genügend Zeit und Handlungsspielraum. Es kann das ganze Unternehmen oder nur ein Bereich überwacht werden, so unterscheidet man auch in strategische oder operative

Prozess	Prozess Schritt	Ziel des Prozess Schritt	Risiko-Nr.	Risiko Beschreibung	Risiko Interdependenzen	Verantwortung
Beschaffung	Bearbeitung und Prüfung der Bestellanforderung	Erfordernis und Anforderung der Bestellung ist zu prüfen.	R1 Bestellrisiko	Der Bedarf liegt nicht vor, Lagerbestände noch da.	Vermeidbarer Aufbau von Beständen (Kapitalbindung) und Reduzierung von Lagerkapazität	Einkauf

Tabelle 3.3: Beispielhafte Risiko-Kontroll-Matrix nach [Diederichs(2012), Abb. 3-11]

Frühaufklärung [Diederichs(2012), S.74-82]. Mehr dazu wird in Abschnitt 3.8 beschrieben.

- Weitere Quellen der Risikoidentifikation können eine ausgiebige **Dokumentanalyse** sein oder der Vergleich von **Kennzahlen, Benchmarks oder Statistiken** nach [Diederichs(2012), S.84].

- **Fehlerbaum-Analysen** sind beliebte Ingenieurwerkzeuge aus der Sicherheits- bzw. Qualitätstechnik um Gesamt- oder Teilsysteme zu analysieren. Sie schaffen eine detaillierte Ursachenanalyse von Geschäftsprozessen, Interdependenzen, kritischen Schwachstellen oder Störungsmöglichkeiten [Denk(2008), S.95].

- **Delphi-Technik** ist eine Prognosemethode bei der externe Experten mehrfach zu ihrer Einschätzung über zukünftige Ereignisse und Trends befragt werden. Ziel ist die frühestmögliche Einbeziehung der Risiken in die Strategie und Planung des Unternehmens [ONR(2014d), 5.2].

Nach [Denk(2008), vgl. S.101-102] ist bereits bei der Risikoidentifikation auf eine passende Dokumentation zu achten, die auch die Ergebnisse der Identifikation beinhalten muss. Dies ist wichtiger Bestandteil einer transparenten Arbeit und für den zumindest jährlich wiederkommenden Risikoprozess unerlässlich. Zum Beispiel um bei rechtlichen Prozessen die Beweislast umzukehren und um weiterfolgende Prozesse von Kategorisierung, Priorisierung, Selektion von Toprisiken und periodische Folgebewertungen mit minimalen Wissensverlust zu gewährleisten.

Abschließend sei erwähnt, dass nur 29% der 1021 vom BDI&PWC befragten mittelständischen Unternehmen mit ihrem Risikomanagement zufrieden sind. Weitere 57% sehen ein leichtes und 12% ein erhebliches Verbesserungspotenzial. 68% sehen obendrein Optimierungspotenzial bei der Risikoidentifikation und -bewertung und somit weit mehr Optimie-

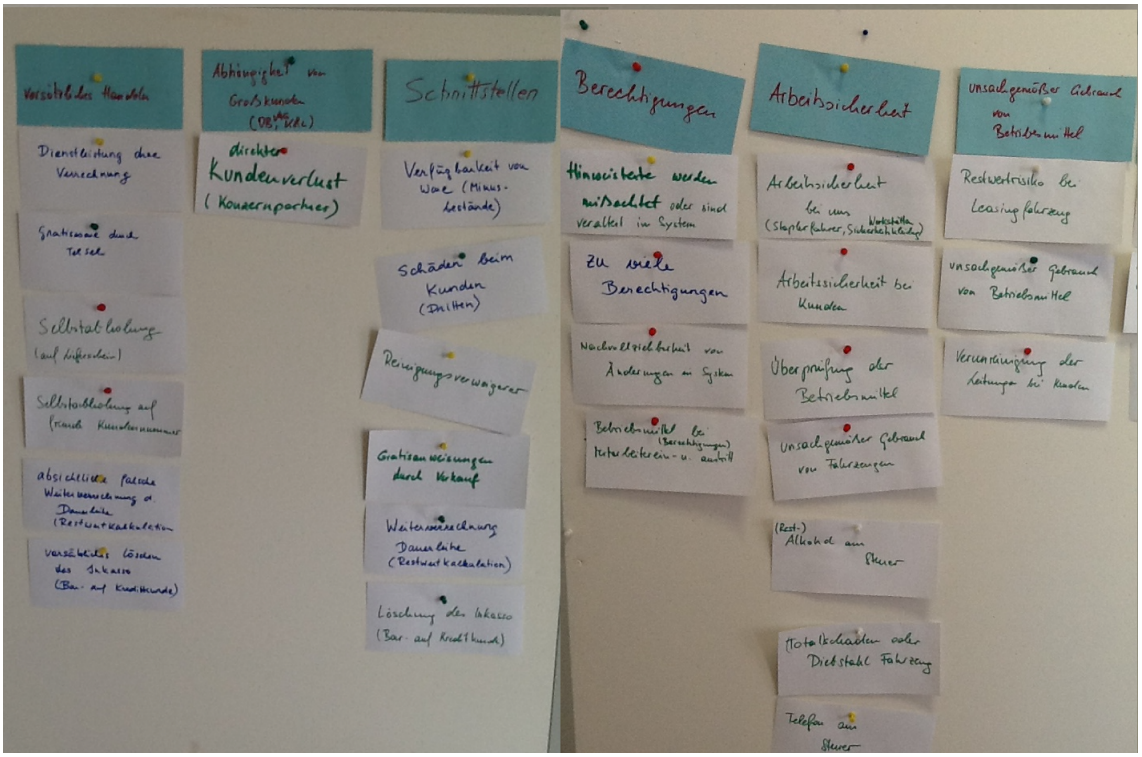


Abbildung 3.6: Beispielhafte Risikoidentifikation und -kategorisierung in einem Workshop

rungspotenzial als im Treasury (25%), Compliance (33%) oder Controlling (48%) [bdi and pwc(2011), S. 24].

Risikoregister bzw. -katalog

Die Risikoklassifikation ist der Abschluss der Risikoidentifikation, also dem Gruppieren von Risiken mit einer gleichen Charakteristik. Es gibt sehr viele verschiedene Möglichkeiten der Einteilung, z.B. nach Risikoquelle, Managemententscheidungen, Zielen, Organisationseinheiten, etc. Hat man sich für eine Einteilung entschieden, stellt dies eine Orientierungshilfe für die jeweilige Risikosituation dar, in der späteren Risikobeurteilung kann mit dieser Klassifikation eine Aggregation stattfinden, [Denk(2008), S.95].

Die Grundeinheit (kleinste Einheit) im Risikomodell ist das einzelne Risikoereignis, an diesem werden alle anderen relevanten Größen wie Prozesse, Daten, Modelle, etc. in der Enterprise-Risk-Management-Software verknüpft. Ein weiterer Grund, aus dem die genauere Einteilung und Verknüpfung der Risiken so wichtig, ist die Weiterarbeit mit Risiko-Berechnungsmodellen, Berichterstattung und Folgewirkungen. Merkmale bei der Kategorisierung von Risiken:

- Es kann ein Risiko im Unternehmen mehrmals und mit verschiedenen Risikoeignern geben, so z.B. Arbeitssicherheit. Für eine große Menge an Risiken bzw. deren Aggre-

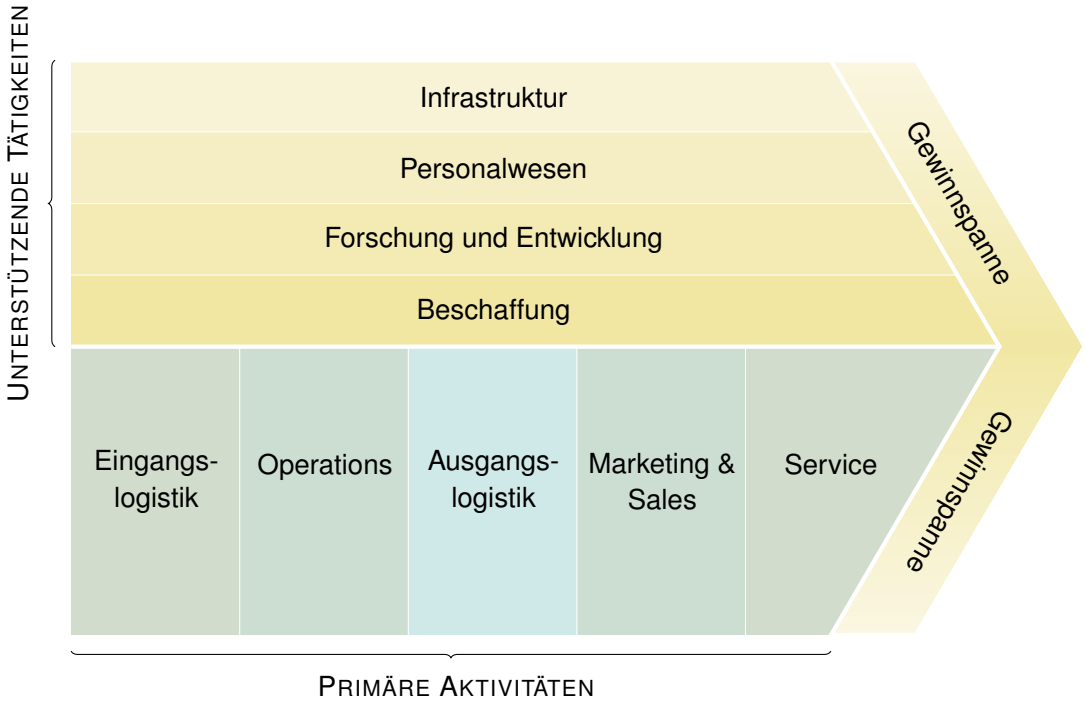


Abbildung 3.7: Risikoidentifikation mittels Wertschöpfungskette nach Porter [Diederichs(2012), S.59]

gation bedarf es eine Unterteilung nach der Organisation wo es auftritt und nach der Art des Ereignisses.

- Risikoarten können gebündelt betrachtet und bewertet werden. Daher muss ein Risikokatalog speziell am Unternehmen angepasst werden.

- Sollte ein Risiko zu mehreren Kategorien passen, wird im Zweifelsfall empfohlen die dominierende Eigenschaft zu nehmen. Mehrfachzuordnungen sind nur für fortschrittliche Unternehmen geeignet, siehe dafür Abschnitt 3.7.

- Pro Risikoart können weitere Merkmale festgesetzt werden, z.B. eine spezielle Methode zur Berechnung oder auch ein eigener Risikoexperte oder Gremium als Verantwortliche.

- Eine häufige Makro-Unterteilung ist jene in externe und interne Risiken. Für die internen Risiken müssen Organisationsstrukturen, Prozesse, Arbeitsplätze, Strategie, Jahresvergleiche und Regelungen im Unternehmen analysiert werden. Bei den externen handelt es sich um jene Risiken die ein Unternehmen nicht verhindern, sondern nur deren Einfluss verringern kann [Diederichs(2012), S.53].

- Laut einer groß angelegten Studie im deutschen Mittelstand werden viele Risikokategorien weitgehend bei Risikoerhebungen berücksichtigt und sind etabliert, z.B. in operative (95 %), strategische (87 %), finanzielle Risiken (87 %), IT (74 %), Compliance (65 %) und Umwelt (58 %) [bdi and pwc(2011), S. 18].

Es gibt keine einheitliche und universal gültige Risikoklassifikation, mehrere Beispiele finden sie im Anschluss. Auch muss erwähnt werden, dass trotz gewissenhafter Kategorisierung, weder ausgeschlossen werden kann, dass Risiken fehlen, noch dass der Prozess der Kategorisierung jemals abgeschlossen sein wird. Eine regelmäßige Überarbeitung ist notwendig, um auf die veränderten Umstände im Unternehmen und deren Umwelt einzugehen [Kaplan and Mikes(06.2012)].

Vorlage für Risikokataloge sind in Fülle vorhanden. Bereits 1995 erstelle The Economist Intelligence Unit gemeinsam mit dem Wirtschaftsprüfer Arthur Anderson einen Risikokatalog [EIU and Arthur-Andersen(1995), S.25ff], der vom “Institute of Chartered Accountants in England and Wales” empfohlen wurde [ICAEW(1997)]. Er beinhaltete folgende drei Kategorien :

- **Umweltrisiken** beinhalten Veränderungen im Wettbewerb, Regulation, Recht, Politik, Stakeholder, Finanzmarkt oder höherer Gewalt
- **Prozessrisiken** mit den Untergruppen Operative- , Technologie-, Integrität-, Finanz- und Empowerment Risiken
  - Operative Risiken beinhalten Betrug, Kundenzufriedenheit, Trademark, Arbeitssicherheit, Lieferkette, Effizienz, Produktentwicklung, Personalwesen oder Umwelt
  - Empowerment Risiken gehen von Führung, Outsourcing, Leistungsanreizen, Change Management bis Kommunikation
  - Technologie Risiken beinhalten Infrastruktur, technologischem Fortschritt, IT
  - Integrität Risiken behandeln Betrug, unauthorisiertes Handeln und Reputation
  - Finanz Risiken decken Preisentwicklungen von Rohstoffen über Zinsen bis Währungen ab, Liquidität mit Cash Flow und Kreditrisiken
- **Informations- und Entscheidungsrisiken** reichen von
  - Betriebsrisiken bei Preisbildung, Performance Management und Regulation
  - Investmentrisiken mit Planung, Budget, Steuer, Finanzberichterstattung bis Buchhaltung
  - Strategierisiken von Geschäftsfeldern, Organisationsstruktur, Produktlebenszyklus bis zu diversen Portfolio Übersichten

Externe-	**Interne Faktoren**
Wirtschaft • Kapitalverfügbarkeit • Kreditvergabe und -verzug • Marktkonzentration • Liquidität • Finanzmärkte • Arbeitslosigkeit • Wettbewerb • Mergers and acquisitions	Technologie • Datenintegrität • Daten- und Systemverfügbarkeit • Systemauswahl • Entwicklung • Verwendung • Erhaltung
Natur und Umwelt • Emissionen und Abfall • Energie • Naturkatastrophen • Nachhaltigkeit	Personal • Fähigkeiten der Mitarbeiter • Dolose Handlungen • Gesundheit und Sicherheit
Politik • Regierungswechsel • Gesetzgebung • Öffentliche Verfahren • Regelungen	Prozess • Kapazitäten • Aufbau und Gestaltung • Durchführung • Lieferantenkette- und -abhängigkeit
	Infrastruktur • Verfügbarkeit des Vermögens • Eignung des Vermögens • Zugang zum Kapital • Komplexität

Tabelle 3.4: Ereigniskategorien nach COSO II [COSO(2009a), Abb. 4.2, Abb. 6.6]

Auch COSO schlägt eine Einteilung der Risiken vor, primär nach internen und externen Faktoren, siehe Tabelle 3.4.

Heute verweisen viele Unternehmensberatungen auf eigene Katalogvorschläge, so teilt die Boston Consulting Group die Risiken in die folgenden Gruppen [Olsen et al.(2011)Olsen, Plaschke, and Stelter, Exhibit 3]. Diese Einteilung wurde auch als Ausgangspunkt für die praktische Umsetzung gewählt, siehe Abschnitt 4.5:

- **Wirtschaftliche Risiken**
  - Marktrisiken mit Rohstoffen, Volumen-Vorhersagen, Marktelastizitäten oder Verkaufsverträgen
  - Kreditrisiken mit Ausfall bei Konsumenten oder Zulieferer
  - Finanzrisiken bei Rating, Cash-Flow, Unternehmenswert, Zinsen, Sicherheit, Verpflichtungen oder Steuern
- **Betriebliche Risiken**
  - Compliance z.B. Gesetze, Ethik und Governance, Verschwiegenheit, Prozessdisziplin, Betrug, Interessenkonflikt, Finanz-Berichterstattungspflichten, Transparenz oder Korruption
  - Operative Excellence z.B. Business Continuity, Führungskräfte, Kundenbeziehungen, Lieferkette, IT, Sicherheit (Security und Safety), Facility-, HR-, Zulieferer-, oder Krisen- Management
  - Umgang mit Anlage- und Umlaufvermögen, betrieblicher Umgang mit Service und Wartung oder singulären Betriebsstörungen
  - Arbeitssicherheit und Umwelt
- **Strategische Risiken**
  - Veränderung von Märkten, Konkurrenz oder Technologien
  - Änderung der gesetzlichen Rahmenbedingungen, Regimewechsel oder Regulation von Markt, Umwelt, etc.
  - Höhere Gewalt und externe Großereignisse z.B. im Markt, Naturkatastrophen, Klagen, Sozio-politische oder in der Lieferkette
  - Geistiges Eigentum (Patente), Spionage, Reputation oder externe Kommunikation
- **Projektrisiken**
  - Planung beim Geschäftsmodell, Zeit- oder Ressourcenplanung
  - Realisierung bezüglich Konzept-, Lizenz- und Transaktionsfehler
  - Passende Integration und Implementierung bezüglich Qualität, Zeit, Kosten und Personell.

Ein letzter lohnender Ansatz ist [ONR(2014c)] der die Gebiete aus dem Projektmanagement direkt für die Risikoidentifikation heranzieht. Beim Risikokatalog muss auf eine so neutral wie möglich gewählte Formulierung geachtet werden. Das hilft sowohl bei der Objektivität, als auch bei der Zuordnung von Chancen, siehe [Denk(2008), S.97].

Spezielle Risikoarten

Da auf die spezifische Risikosituation des Unternehmens einzugehen ist, müssen bei der Ermittlung relevanter Risiken auch Branchen- und organisatorische Eigenheiten beachtet werden, anbei einige Beispiele:

- Die eher selten erwähnten **Familienrisiken** sind gerade in der mittelständischen Unternehmenslandschaft in Zentraleuropa wichtig. Durch die Überlappung von unternehmerischer und familiärer Sphäre sind Vorkehrungen nötig, die es bei anderen Unternehmensformen nicht braucht. Diese Vorkehrungen betreffen die Nachfolgeregelung oder Familienzusammenhalt durch Familienrat oder -verfassung. Speziell für österreichische Familienunternehmen findet man in [Maissner(2010)] in Abschnitt 4.9 eine umfangreiche Studie.

- **Endogene Risiken durch Regulierungen und Leitfäden**. Diese Risiken entstehen durch die hohen Kosten, die durch die Umsetzung von komplexen Regulierungen entstehen. Das ist ein gängiger Kritikpunkt bei Risikomanagementleitfäden wie Basel oder Kontrag. Durch regulierte und damit einheitliche Systeme entstehen ebenfalls Risiken, da sich ein Herdentrieb entwickeln kann oder Systemfehler überproportional verstärkt werden können [McNeil et al.(2015)McNeil, Frey, and Embrechts, S. 28, 31].

  Schließlich können inoffizielle defacto Standards wie fair-value Bewertungen und marktkonsistente Bewertungen prozyklisch wirken und haben neben ihren guten Transparenzeigenschaften auch Risiken. Ein Beispiel hierfür wäre gewissermaßen die Finanzkrise 2007-09 [McNeil et al.(2015)McNeil, Frey, and Embrechts, S. 28].

- Eine weitere im deutschsprachigen Raum selten beachtete Risikokategorie sind die **Risiken durch Verträge**. Verträge sind in der neuzeitlichen, privatisierten und auslagernden Marktwirtschaft nicht mehr wegzudenken [Cruz(2004), S. 26ff].

- Einer Studie nach [BFI(2006), S.34] zufolge, berichten 48 börsennotierte, österreichische Unternehmen zwischen 2002 und 2004 durchschnittlich 3,52 (2002) bzw. 5,56 (2004) Risikokategorien. Die externen Risiken überwogen deutlich vor den Internen. Die häufigsten Nennungen betrafen Finanzrisiken wie das Währungsrisiko mit 52%, Kreditrisiko 48%, Vertriebsrisiko 40% und Zinsrisiko 33%. Daraus lässt sich folgern, dass die befragten Unternehmen damals nicht gewillt waren ihre interne Risikoposition vollständig preiszugeben und das RM generell noch einen primitiven Status aufwies. Bei [bdi and pwc(2011), S. 12]. wiesen bereits 70% Konjunktur und Wettbewerb als größtes Risiko aus, gefolgt von Gesetzvorhaben 63%, Fachkräftemangel 58%, Finanzrisiken 43% und Steuerrisiko 26%.

- Neben den Makrorisiken, die prinzipiell für alle Unternehmen gelten, sind auch Systemrisiken für Finanz- oder Absatzmärkte nicht zu vergessen, [McNeil et al.(2015)McNeil, Frey, and Embrechts, S.15] . Gewisse kurzweilige Modeerscheinungen sind in Zeiten großer Skandale (also materialisierter operativer Risiken wie Betrug) oder nach höheren Naturgewalten durchaus zu beobachten. Es liegt auf der Hand, dass diese besser langfristig und systematisch behandelt werden sollten.

- Laut [bdi and pwc(2011), vgl. Kp. 5 und 6] ist die **Vernachlässigung von Querschnittsthemen** eine latente Bedrohung. So sollen z.B. alle Unternehmensbereiche im RM mit einbezogen werden und nicht nur ausgewählte Tochtergesellschaften oder Beteiligungen. Denn gefährliche Toprisiken können durch Verkettungen von banalen Ereignissen oder mehreren korrelierten Einzelrisiken entstehen.

- Die **IT Risiken** sind in aller Munde und Abschätzungen diesbezüglich ein riesiges Themenfeld. Einen ersten Anhaltspunkt bietet das Unternehmen Sans, es bewertet jährlich die technischen Risiken von tausenden Unternehmen und packt diese in Listen. [7]. Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt ein Datenblatt mit IT-Sicherheitsanforderungen, Anforderungskatalog, IT-Grundschutzkatalogen und IT-Sicherheitskonzept zur Verfügung [8].

3.7 Risikobeurteilung

Zusammenfassung der Risikobeurteilung [Denk(2008), vgl. S.102-104] :

Das ist Die Risikobeurteilung versucht die zuvor identifizierten Risiken mittels Szenarios, Frequenz und Konsequenz zu bewerten, vorzugsweise quantitativ oder mindestens qualitativ. Um Risiken zu managen müssen sie zuerst gemessen werden! Abschließend werden Verbindungen und Aggregationen zwischen den Risiken vorgenommen.

Grundlage Die Ergebnisse der zuvor stattfindenden Risikoidentifikation liegen in Form von Risikoinventaren, Risikoquellen und Kategorisierung vor, siehe Abschnitt 3.6.

Kriterium 1 Objektivität, die bei quantifizierbaren Risiken mittels Datensammlungen oder bei schwach dokumentierten Ereignissen mittels qualitativer Einschätzung in Worten erfolgen kann. Eine qualitative Skala reicht beispielsweise von schlecht, passend, gut bis ausgezeichnet. Eine schriftliche Dokumentation über solche Grundannahmen sollte dabei sein.

Kriterium 2 Vergleichbarkeit der Ergebnisse durch einheitliche und definierte Methoden.

[7] http://www.sans.org/top25-software-errors/ oder http://www.sans.org/critical-security-controls (24.02.2014)

[8] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html;jsessionid=FB7DD94F1BA0D04EBBEEAC4EB802034D.2_cid286 (24.02.2014)

$Kriterium\ 3$ Quantifizierung, dadurch können automatisierte Abweichungen zwischen Plan- und Ist-Größen ermittelt werden und Aggregation durchgeführt werden. Sollte dies während der Einführung nicht möglich sein, reicht erstmalig eine qualitative Schätzung und kann künftig im Prozess der Folgeperiode nachgeholt werden.

$Kriterium\ 4$ Berücksichtigung von Interdependenzen, also dass zum Bespiel mehrere Risiken die gleiche Quelle haben können. Dies sind Kettenwirkungen in denen Risiken als Folge anderer Risiken auftreten. Es sind auch kumulative Wirkungen, in denen erst durch zwei gleichzeitig eintretende Risikoquellen ein Risiko entsteht. Verkehrt proportional verhält es sich mit Kompensationseffekten mehrerer banaler Einzelrisiken, die in eine glückliche Auflösung dieser Risiken münden.

$Ziel\ ++$ Der Aufbau von Detailwissen und Verständnis über die eigenen Risiken zu erhalten.

$Ziel\ +$ Die ursächlichen Strukturen und diverse Abhängigkeiten von Risiken transparent zu machen und ihre möglichen Auswirkungen schlussendlich mit Zahlen zu belegen.

$Nachfolge$ Die Steuerung von Risiken mittels passenden Maßnahmen, um sie dem Risikoappetit entsprechend auf ein ertragbares Maß zu reduzieren, siehe Kapitel Abschnitt 3.8.

Ansätze zur Risikobeurteilung

Nach ISO31000 beinhaltet die **Risikobeurteilung** die Risikoanalyse und Risikobewertung. Die Risikobewertung kann wie jede andere Bewertung grundsätzlich mit Hilfe quantitativer und qualitativer Maße erfolgen (hier im speziellen Risikomaße). Die erste Frage bei der Messung ist, wogegen kann man messen und die zweite Frage ist die nach den Zielwerten und Toleranzen dieser Messung. Die quantitative Risikobewertung nach [Denk(2008), vgl. S.103-104] findet mittels Zahlenwerten in EUR oder Wahrscheinlichkeiten in % statt. Sie ist in der Regel aufwendiger. In der Praxis können verschiedene Methoden für die Ermittlung vom wahrscheinlichen Schadensausmaß, Eintrittswahrscheinlichkeit, Eintrittsfrequenz oder Wahrscheinlichkeitsverteilungen eingesetzt werden, siehe [Denk(2008), vgl. S.103-106]:

- Generell können Bewertungsverfahren nach Art der zu ermittelnden Risikoparameter in quantitative, semi-quantitative und qualitative eingeteilt werden. Quantitativ bedeutet den Einsatz einer metrischen Skala. Qualitativ setzt eine verbal beschriebene Skala ein. Semi-quantitativ ist eine Kombination aus beidem, durch Verwendung eines verbal beschriebenen und gleichzeitig quantitativ beschrifteten Wertebereich [Diederichs(2012), S.90].

- Das einfachste **quantifizierte Risikomaß** ist ein Erwartungswert durch Multiplikation der geschätzten Schadenhöhe mit der geschätzten Eintrittswahrscheinlichkeit. Diese Expertenschätzung ist in der Praxis weit verbreitet, vor allem bei der Ersteinschätzung [Romeike and Hager(2013), vgl. S.115]. Die **Schätzung von Werten** hat als Nachteil, dass sie eine Verdichtung ist und gegenüber einer Risikoverteilungsfunktion einen Informationsverlust hat. Die Schätzung reduziert den Ereignisraum auf 2 Zustände, dem Eintritt in voller Höhe oder den nicht Eintritt.

- Somit ist für das nächstbeste quantifizierbare Risikomaß direkt die Wahl einer **Verteilungsfunktion** heranzuziehen, die alle möglichen Zustände abbildet, aggregierbar ist und Interdependenzen ermöglicht. Die Wahl der Verteilungsfunktion ist entscheidend, entweder lässt man sie durch Experten schätzen oder man kann sie durch Daten belegen. Beispiele für Verteilungsfunktionen sind die Dreiecksverteilung mit minimalen, durchschnittlichen und maximalen Wert, die Normalverteilung bei VaR oder die Binomialverteilung als Zufallsverteilung [Romeike and Hager(2013), vgl. S.115-118].

- Die verschiedenen **Bewertungsskalen** richten sich in Relation zur Organisation und ihrer Ziele, [pwc(2008), S.15]. So bleibt einem Unternehmen mit wenig auswertbaren bzw. quantifizierbaren Daten nichts anderes übrig als qualitative Skalen zu verwenden. Generell sollten im Unternehmen anpassbare Skalen zum Einsatz kommen, damit in verschiedenen Unternehmensbereichen auf die dortigen Umstände eingegangen werden kann. Beispielsweise werden Bedeutungsskalen der höchsten Risikostufe bei Abteilungen mindestens eine Zehnerstelle weniger aufweisen (z.B. 100 TEUR), als das fürs gesamte Unternehmen der Fall ist (z.B. 1.000 TEUR). Trotz unterschiedlicher Zehnerstelle lassen sich diese quantifizierten Skalen jedoch wieder aggregieren [Shenkir and Walker(2007), S.14].

- Bei der **qualitativen Risikobewertung** werden passende Kriterien herangezogen, um das Ausmaß eines Risikos zu beurteilen. Bei Eintrittswahrscheinlichkeit kann dies von selten (alle 100 Jahre), manchmal (alle 20 Jahre), oft (alle 5 Jahre) bis sehr oft (alle 2 Jahre) reichen. Beim Schadensausmaß kann dies von unbedeutend (0-5% Umsatz), bedeutend (über 5% Umsatz), schwerwiegend (über 25% Umsatz) bis existenzgefährdend (über 100% Umsatz) reichen [Denk(2008), vgl. S.106]. Bei der Einteilung und Benennung dieser Skalen sind der Kreativität keine Grenzen gesetzt. Um Verwirrungen zu verhindern sollte die Gesamtzahl verschiedener Skalen im Unternehmen begrenzt sein. Der prinzipielle Aufbau sollte unternehmensweit abgestimmt sein, z.B. die Anzahl der Unterteilungen, die einheitlichen Normeinheiten und Dimensionen wie Tausend oder Million. Skalen die gerade Unterteilungen von 4 oder 6 Stufen haben, erschienen sinnvoll, da keine sogenannte goldene Mitte existiert.

- Die Risikobeurteilung soll an der untersten Ebene erfolgen und erst dann durch Aggregation in einen unternehmensweiten Rahmen gebracht werden [Shenkir and Walker(2007), vgl. S.11].

Die **Risikoanalyse** nach [Denk(2008), vgl. S.107-126] ist der zweite Teil der Beurteilung und dient der Gewinnung eines Verständnisses über die Risikosituation. Dabei sind vielfältige Methoden im Einsatz wie im nächsten Abschnitt 3.7 geschildert.

In Verwendung sind Simulationen mittels historischer oder zufallsgenerierter Datenreihen (Monte-Carlo Simulation), Modelle mit Differentialgleichungen (Weltmodell), Scoringmodelle, Entscheidungsbäume, Regressionsanalyse, Szenarioanalyse oder grafische Risikomatrizes [Damodaran(2008), Kp.5, 6 und 7]. Den Abschluss des Kapitels bildet die Aggregation und die damit betroffene Frage von Interdependenzen (auch Korrelationen genannt).

Das Management benötigt Aggregation, meist in Form einer Portfolio Ansicht der Risiken, um als Entscheidungsgrundlage zu dienen, [pwc(2008), S.15]. Die Aggregation muss aufteilbar, nach verschiedenen Risikokategorien und Organisationsebenen sein. Damit der Risikomanagementprozess und die Planungswerte nach belieben pro Abteilung, pro Risikokategorie, pro Risikoeigner oder fürs ganze Unternehmen ausgewertet werden können!

Methoden zur Risikobeurteilung

Methoden zur **Risikobeurteilung** schließen nach ISO31000 sowohl die Risikoanalyse als auch Risikobewertung mit ein. Fast alle Methoden wie sie in der Übersicht Tabelle 3.2 aufgelistet und bewertet sind, können für mehrere Schritte im Risikomanagementprozess verwendet werden. Im folgenden Abschnitt wird detailliert auf die Fähigkeit ausgewählter Methoden zur Risikobeurteilung eingegangen. Bei der Umsetzung von Modellen muss auf ein passendes Back-testing und Stress-testing zur Qualitätskontrolle geachtet werden. Kein Risikomaß ist perfekt, darum müssen ausführlich alle Vor- und Nachteile bedacht werden [Romeike and Hager(2013), vgl. S.119-122]:

- Die **Expertenschätzung von Eintrittswahrscheinlichkeit und Schadensausmaß**, ist das einfachste qualitative und quantitative Verfahren zur Bewertung von Risiken. Ein Beispiel ist in Abbildung 3.8 gezeigt. Die Nutzung dieser Methode ist oft bei der Einführung des Risikomanagements oder beim Fehlen von Daten zu einem neuen Problem nötig. Daher sind subjektive Einschätzungen von internen und externen Experten oder Expertengruppen möglich. [Diederichs(2012), S.89ff].

- **Sensitivitätsanalyse**, ist der Aufbau eines Modells mit einfachen Formeln in denen mehrere Variablen variiert werden können. Damit können grobe Abschätzungen möglicher künftiger Entwicklungen und Situationen durch Änderung einfacher Kennzahlen erhalten werden. Diese Abschätzungen sind ungenau, aufgrund der Vereinfachungen bei der Variablenzahl und deren gegenseitige Abhängigkeiten. Praxisnahes Beispiel ist die Analyse des Konzernumsatzes mit verschiedenen Rohstoffpreis- und Wachstumsprognosen. Die Einfachste Form ist die Analyse einer einzelnen Kennzahl und ihres Hauptrisikofaktors, [Denk(2008), vgl. S.107].

- **System Design**, diese Simulationsart wurde durch die Veröffentlichung des Weltmodells von J. W. Forrester und dem Club of Rome berühmt. In ihrer Idee ist es eine kompliziertere Sensitivitätsanalyse. Dabei simuliert man mittels Differentialgleichungen die Entwicklung von Bevölkerung, Wirtschaft und Umweltbelastung und entwickelt Szenarien und Prognosen für eine künftige Welt. In Abbildung 3.9 wird dies mittels Variablen wie Geburten-, und Sterberaten, Wirtschaftswachstum, Wirtschaftsziele, Umweltverschmutzung und -Regeneration erreicht. Diese Disziplin wird heute System Dynamics genannt, siehe [Forrester and Forrester(1971)] und [Sterman(2000)].

- Die **Szenariotechnik** oder auch Delphi-Methode stammt aus der Unternehmensplanung. Sie skizziert mit oder ohne Experten einen Sachverhalt ausgehend von der

Gegenwart auf zukünftige Entwicklungen, inklusive alternativen Rahmenbedingungen [Romeike and Hager(2013), vgl. S.112].

- **Entscheidungsbäume** bieten eine Analyse durch den Aufbau einer Struktur, wie es in FMEA, fault-tree oder event-tree [Damodaran(2008), vgl. S.153ff] geschieht. In diese Kategorie fallen auch die graphentheoretische-analytische Methoden nach [Denk(2008), vgl. S.114-115] und [Damodaran(2008), vgl Fig.6.1-6.3].

- Die Ermittlungen von **Verteilungsfunktionen** einzelner Risikokategorien ist bei fortschrittlichen Risikoquantifizierungen notwendig [Romeike and Hager(2013), vgl. S.113ff]. Rohdaten sind selten so schön verteilt wie es für die meisten Verteilungen notwendig wäre. Es ist eine eigene statistische Disziplin die Rohdaten in passende Verteilungen zu bringen und passende Kompromisse zu finden (engl. fitting). Es ist häufige Praxis für nicht normal verteilte Risikoarten, dann doch die einfacher berechenbare Normalverteilung heranzuziehen. Wenn die Daten nicht den Kriterien einer Normalverteilung entsprechen, sollte man auch eine für die Risikoart besser passende Verteilung verwenden, [Damodaran(2008), vgl S. 199]. Eine Auswahl an Verteilung inklusive Entscheidungshilfe wird in Abbildung 3.10 gezeigt. Beispielsweise haben Währungs- und Rohstoffpreisrisiken Normalverteilung, gesetzliche Regulierungsänderungen Dreiecksverteilung oder Umweltverschmutzungen durch Pipelinelecks Log-Normalverteilung [Popescu(2014), F. 14].

- Eine **Jahresabschlussanalyse** kann nach [Diederichs(2012), S.103] eine passende top-down Methode zur Analyse von Risiken darstellen.

- **Scoring-Modelle** verwenden eine Zuordnung von festgelegten Wertungspunkten, um mehrere Risiken aus einer homogen oder heterogen zusammengesetzten Gruppe qualitativ zu vergleichen und priorisieren. Eine stark vereinfachte Aggregierung ist ebenfalls möglich. Es ist die einfachste unter den systematischen und nachvollziehbaren Bewertungsmethoden, siehe [Denk(2008), S.198]. Ein Beispiel ist in Abbildung 3.8 abgebildet.

  An Vorkenntnissen und Gruppenzusammensetzungen sind keine Ansprüche gestellt. Zudem können pro Risiko mehrere Kriterien gleichzeitig bewertet werden, wie Eintrittswahrscheinlichkeit, Schadensauswirkung, Entdeckbarkeit, Messbarkeit oder Dringlichkeit. Nachteile sind, dass subjektive Präferenzen manipulieren oder gar dominieren können. Die Gefahr von scheingenauen oder unreifen Beurteilungen schwächen die langfristige Glaubwürdigkeit dieser Methode. Bei initialer Einführung eines Risikomanagements ist sie gut geeignet, bei reiferen Unternehmen sollte sie jedoch schnell abgelöst werden, [Diederichs(2012), S.97-102].

- **Risikoportfolioanalyse** mit einer sogenannten Risikomatrix bzw. -landkarte (engl. riskmap) ist eine einfache Methode, um Risiken nach mehreren Kriterien zu filtern oder aggregieren. Beispiele sind in Abbildung 4.9, Abbildung 4.10 und Abbildung 4.15 zu sehen. Zum einen steht ein zweidimensionales Koordinatensystem zur Verfügung, bei dem die Kriterien nach potentieller Schadenshöhe und Eintrittswahrscheinlichkeit

aufgetragen werden. Weitere Darstellungskriterien der Risikolandkarte, z.B. Risikokategorie oder Organisationseinheit können mittels Filter ausgewählt werden. Es handelt sich bei diesem Verfahren um einen raschen Überblick über die Risikosituation des Unternehmens. Da die Risiken ausdrücklich keine quantitativen Daten benötigen, sondern bereits qualitative Expertenschätzungen ausreichen, [Denk(2008), vgl. S.119-123].

- Die **value-at-risk und artverwandte Methoden** sind ein Schätzwert, der mit einer einzigen Zahl beschreibt, das der maximale Verlust einer einzelnen oder aggregierten Risikoposition bei normalen Marktbedingungen nicht das gewählte Konfidenzniveau von 95, 99 oder 99,9 % überschreitet [Denk(2008), vgl. S.107]. Der value-at-risk (kurz VaR) nutzt historische oder zufallsgenerierte Datenreihen [Damodaran(2008), vgl. S.164ff] um Konsequenzen von Änderungen zu verstehen. Die historischen Daten werden unter anderem genutzt für value-at-risk Werte oder Varianz-Kovarianz-Modelle. Zufallsgenerierte Datenreihen dienen der Monte-Carlo Simulation. Das aus der Finanzbranche stammende Risikomaß VaR wurde von JP Morgan 1989 innerhalb des selbstentwickelten Risikomanagementansatz "RiskMetrics" [9] erfunden. Weitere Details sowie alternative Kennzahlen wie expected-shortfall oder cashflow-at-risk sind im Abschnitt 3.7 beschrieben.

- Die **Fundamentalgleichung der Risikobewertung nach Gleißner** ist eine Methode zur Aggregierung des Gesamtrisikos im Unternehmen. Dabei werden die Kategorien Leistung- und Marktrisiko dreistufig beurteilt (kritisch, gefährdet und OK) und addiert. Abschließend wird dies mit zwei Faktoren multipliziert, den Fixkostenanteil und den Verschuldungsgrad. Details siehe [Gleissner(2011), vgl. S.175-180].

- Eine Inspirationsquelle finden Risikomanager in den Produktentwicklung- und Qualitätsmanagement Abteilungen der traditionellen Industriekonzerne, sowie der Sicherheitsindustrie (Safety Engineering und Functional Safety). Insbesondere die japanischen Kaizen Produktionsphilosophien sind durchzogen von Risikobewusstsein und robusten Unternehmensprozessen auf allen Ebenen des Unternehmens.

- Eine sehr übersichtliche und initiale Risikobewertung kann nach den **[Curtis and Carey(2012)] Methoden** erfolgen.

- **Betriebswirtschaftliche Methoden für die Risikobewertung**

  - discounted-cashflow-approaches bieten die Möglichkeit mittels Abzinsung die künftig verfügbaren Zahlungsüberschüsse (engl. cashflow) zu berechnen. Dies bietet auch die Möglichkeit die Liquidität zu planen [Damodaran(2008), vgl. S. 98ff] und eine Zahlungsunfähigkeit zu vermeiden. Auch dafür bedarf es Verfahren zur Aggregation von Risiken. Zur Abzinsung wird der WACC (weighted-average-costs-of-capital [DGR(2008), S.11]) verwendet, dieser Zinssatz orientiert sich am Ertrag aller anderen Investmentmöglichkeiten.

[9] `http://www.jpmorgan.com/RiskMetrics/RiskMetrics.html` (24.02.2014)

  - Beim EVA-Ansatz (economic-value-added) ist eine wertsteigernde Unternehmensleistung definiert als Residualgewinn nach Abzug von Kapitalkosten. Anders erklärt, EVA ist ein höherer bilanzieller Erfolg gegenüber der Verzinsung des eingesetzten Kapitals mittels WACC [Romeike and Hager(2009b), vgl. S.106].
  - Gängige Kennzahlen können für die Risikoquantifizierung oder Frühwarnung herangezogen werden, darunter fallen u. a. Kauffähigkeit pro Kunden, Zurückweisungsquote, profitabelste Kundenbeziehungen, Umsatzanteil Topkunden, Einheiten pro Einkauf, Akquisitionskosten je Neukunde oder Kundenwert [10]. Weitere Details siehe Abschnitt 2.4 oder Tabelle 3.7.

- Die Bewertungsmethoden in den **Baseler Akkorden I,II und III** sind für die Finanzbranche entwickelt worden. Für sehr fortgeschrittene, industrielle Risikomanagementsysteme oder in Spezialbereichen, wie dem Rohstoffhandel sind sie teilweise auch für die Industrie umsetzbar. Es gibt einige ausgefeilte Methoden für eine projektabhängige Absicherung mittels Risiko-Eigenkapital.

  - Basel 3 hat 3 Säulen engl. pillars, auf denen nach deren Sicht die Regulierung von Finanzinstituten beruht, die minimalen Eigenkapitalanforderungen (engl. capital-requirement), die Aufsicht (engl. supervisory-review-process) und die Marktdisziplin (engl. disclosure).
  - Die in Basel 3 geforderten Kapitalanforderungen sind mittels einzuhaltender minimaler Eigenkapitalquote (engl. capital-ratio) geregelt. Diese berechnet sich durch Division von Eigenkapital durch risk-weighted-assets (RWA). Um eine konforme und komfortable Eigenkapitalquote zu erhalten, kann nun das Eigenkapital erhöht oder der RWA optimiert werden. Die RWA Optimierung erfolgt in den Risikomodellen, Prozessen, counterparty-credit-risk, Geschäftsmodellen, Portfoliooptimierungen, Besicherungsmanagement (engl. collateral), IT-Infrastruktur oder Datenqualität [accenture(2013), F. 28].
  - Weiters führte Basel 3 neue Methoden ein, u. a. zur Beschränkung des maximalen Fremdkapitalhebels (engl. leverage), der Liquiditätsberechnung, der Kernkapitalberechnung und des counterparty-risk bei Derivaten [McNeil et al.(2015)McNeil, Frey, and Embrechts, S.18].
  - Bei der Ermittlung von operationellen Risiken sind drei Methoden (Standard-, Basisindikator- oder fortgeschrittener Ansatz (AMA)) nennenswert. Basel erstellt und bereitet Datenmaterial auf, in dem unternehmensübergreifende, gemeinsame OpRisk Schadensfalldatenbanken verpflichtend befüllt werden müssen, sogenannte quantitative-impact-studies (kurz QIS) [11].
  - Zusammenfassend sind die Baseler Akkorden ein derzeitiger Stand der Technik, bei dem sich weder Manager noch Kontrolleure vollends auf alle Methoden verlassen sollten, es ist ein work-in-progress! Deswegen veranstaltet das Basel

[10] `http://kpilibrary.com` (24.2.2014)
[11] `https://www.bis.org/bcbs/qis/` (20.10.2015)

Committee alle paar Jahre ein joint-forum, dessen Publikationen beispielsweise folgende Kritikpunkte bei der Aggregierung von Risiken beinhalten:

  * Die Finanzkrise die 2007 begann, brachte, zumindest in einem gewissen Grad, ein Versagen der Methoden zur Risikoaggregation zum Vorschein. Es hat erstaunlicherweise wenig Bewegung bei den meisten dieser Unternehmen gegeben, ihre Aggregationspraktiken signifikant zu revidieren oder zu überarbeiten [Basel(2010b), vgl. S.4]!
  * Zu denken gibt der Umstand, dass die ausgewählten Methoden oft eine mathematische Struktur bleiben und in einem Vakuum betrieben werden, wenn sie nicht tief in die Unternehmensbereiche und Management integriert und verankert werden [Basel(2010b), vgl. S.5].
  * Finanzunternehmen versuchen üblicherweise durch gemessene Diversifikationseffekte ihrer internen Risikoaggregationsmethoden die Kapitaldeckungen zu verringern. Jedoch brauchen verlässliche Messungen von Diversifikationseffekten auch verlässliche Risikomessungen, insbesondere in den Enden der Verteilung (engl. tails of distribution) [Basel(2010b), vgl. S.5].
  * Generell erheben die meisten Supervisor den Anspruch, nicht im großen Umfang auf die aus internen Modellen ermittelten Kapitaldeckungen und Diversifikationseffekten zu vertrauen. Sie werden als interessante work-in-progress angesehen, vor allem da die meisten Aggregationsmodelle ursprünglich nicht für die Kapitaldeckung entwickelt wurden. Wegen der großen Herausforderungen die Finanzunternehmen bei ihren internen Modellen haben, den Verweis auf deren bisherige Leistungen und wegen der generell skeptischen Einstellung der Supervisor wird ein abwägender und wachsamer model-based-approach empfohlen. Interne Modelle zur Erkenntnisgewinnung gelten als angemessen [Basel(2010b), vgl. S.6] .

– Die deutschen Sparkassen veröffentlichen regelmäßig einen Leitfaden mit den Mindestanforderungen, dort werden Aufsicht, Prozesse, technische- und personelle Anforderungen, Risikotragfähigkeit, Risikosteuerung, interne Revision, Compliance und vieles mehr beschrieben [MaRisk(2014), S.1ff].

– Oprisk können dabei durch Schadensfalldatenbanken, Risikoinventurlisten, Risikolandkarten, Oprisk-Pool und operationellle VaR behandelt werden [MaRisk(2014), Abb. 80]. Da die Oprisk Management Methoden nicht zwingend vorgeschrieben sind, können z.B. auch risk-control-and-self-assessment (RCSA) oder key-risk-indicators (KRIs) verwendet werden.

– Die deutsche Bankenaufsicht erstellt ebenfalls Leitfäden und beurteilt Methoden. Beispielsweise behandelt [BaFin(2011), S.1ff] das Risikodeckungspotenzial, Risikoarten und Risikoquantifizierung.

Eine managementfreundliche und zufriedenstellende Methode, Ereignisse im Unternehmen mit ihrer Risiko- und ihrer Chancenseite zu betrachten ist ein Tornado Diagramm wie in Abbildung 3.11 gezeigt.

Abbildung 3.8: Beispielhafte qualitative Risikobewertung mit der Scoring Methode während einem Workshop

Betrachtet man die gängigsten Methoden so lassen sich vier wesentliche Aspekte bzw. Fragestellungen nach [Wengert and Schittenhelm(2013), S. 36] erkennen:

1. “Die Stärke von Preis- und Wertänderungen,
2. der Grad des Matchings von cashflows,
3. die Ausfallwahrscheinlichkeiten und
4. die Ermittlung von Gesamtrisiken.”

Nach [Wengert and Schittenhelm(2013), vgl. S. 36ff] beschäftigt sich die erste Klasse mit Vermögenswerten und wie sich diese wertmäßig verändern. Als einzelnes Risikomaß dient die Preissensitivität. Die zweite Klasse beschäftigt sich mit zukünftigen Zahlungsströmen, die dritte Klasse verwendet statistische Werkzeuge, darunter fällt auch das value-at-risk (VaR) Risikomaß. Die vierte Klasse an Methoden beschäftigt sich mit dem Gesamtumfang von Risiken und beinhaltet Methoden die Abhängigkeiten und Korrelationen zwischen den Risiken bzw. Risikoklassen abbilden.

Andere Einteilungsmöglichkeiten wären etwa die Unterteilung in Indikator- (Basel, BSC, Frühwarnung), Befragungs- (z.B. Szenario), Technische-(Entscheidungsbäume), Finanzma-

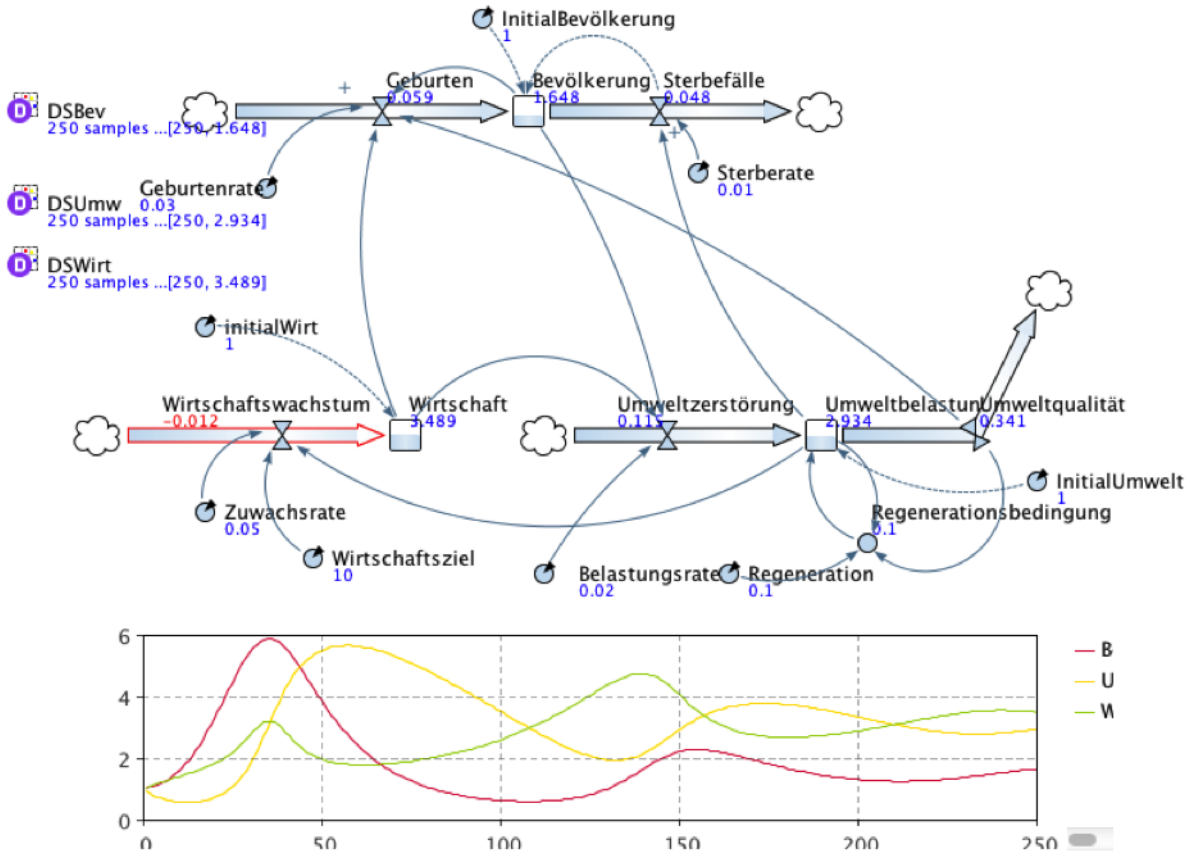


Abbildung 3.9: Beispiel für eine klassische Weltmodell Simulation nach Forrester mittels Anylogic 3.8 Software

thematische (RiskMetrics)- oder stochastische Methoden (Monte-Carlo). Die Einteilung dieser Methoden wird im Zuge dieser Arbeit nicht näher untersucht, da dies ein eigenes Spezialgebiet ist.

Risikoquantifizierung als Bestandteile der Analyse

Bei der Risikoquantifizierung geht es primär um eine nachvollziehbare Abschätzung von Risiken. Dabei steht man schnell vor dem “KuU-Dilemma” nach [Diebold et al.(2010)Diebold, Doherty, and Herring, S.2-3]. Dies steht für:

- K (engl. Known) als bekannte Zufallsphänomene von denen man Wahrscheinlichkeitsverteilung und Prozesse kennt,
- u (engl. unknown) sind Phänomene die man sich erklären aber keine Aussagen zur Wahrscheinlichkeit treffen kann und

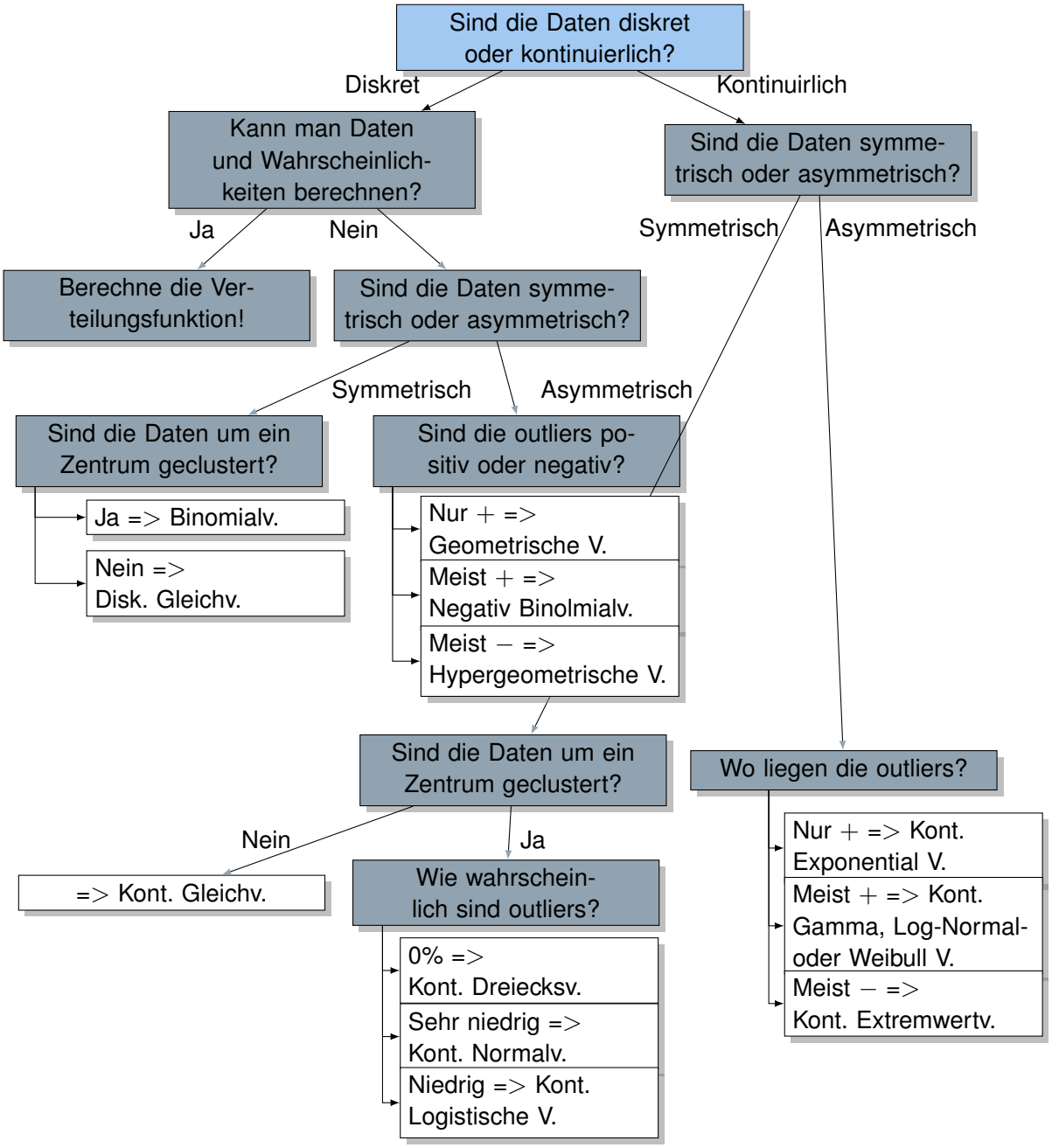


Abbildung 3.10: Bewertung mittels verschiedener Verteilungsfunktionen nach [Damodaran(2008), S.200, Figure. 6A.15]

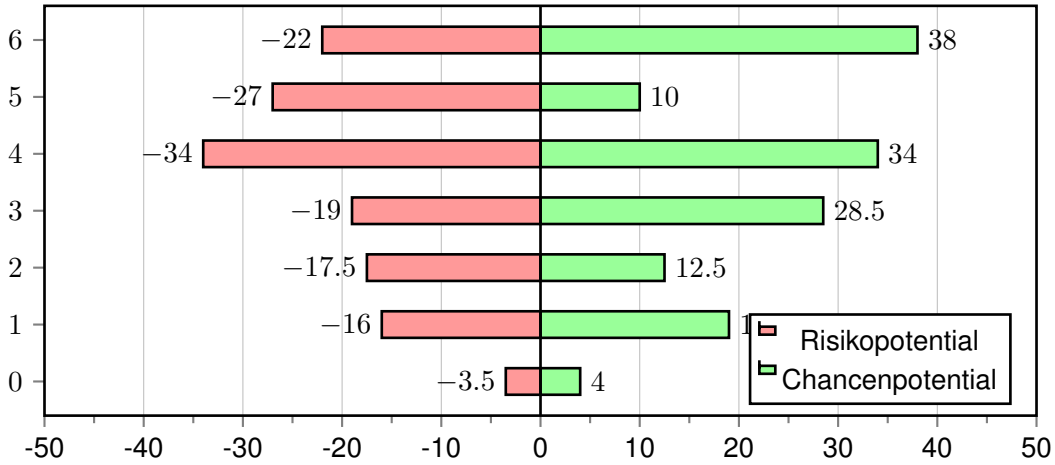


Abbildung 3.11: Beispielhafte Darstellung eines quantifizierten Ereignisses mit einem Tornado Diagramm

- U (engl. unknowable) sind völlig neue und ungeordnete Phänomene im Risikomanagement.

Die derzeitige Situation bei der Quantifizierung:

- Ein wesentlicher Schritt der Risikoquantifizierung ist eine entsprechende Datenbasis, also die Messung von Daten und deren Datensammlung. Bei der Messung sind verschiedene Verfahren möglich. Als Hinweis kann man sich durchaus an der Qualitätsmessung bei Dienstleistungen orientieren. Diese sind in subjektive und objektive Verfahren unterteilbar [12]. Objektive Verfahren sind z.B. Testkäufe, Beobachtungen oder Messungen quantifizierbarer Unternehmenszahlen. Subjektive Verfahren gliedern sich in merkmalorientierte, ereignisorientierte und problemorientierte Verfahren. Darauf wird in dieser Arbeit nicht näher eingegangen.

- Das Problem unzureichender Schadensdaten ist für alle mathematisch-statistischen Risikoanalyseverfahren gravierend. Ein Risiko kann nur richtig mit einer ausreichenden Anzahl zuverlässiger Daten quantifiziert werden. Bei einigen Risikokategorien, z. B. bei Marktrisiken, ist das gegeben. Bei anderen Risikokategorien in der Industrie oder operationellen Risiken ist die Datensituation schlecht. Der Grund liegt darin, dass Schadenfälle bisher nur dann gemeldet wurden, wenn sie nicht vertuscht werden konnten. Beinaheschäden oder mögliche Risiken werden auch kaum quantifiziert erfasst. Um aussagekräftige Verlustdatenbanken zu erhalten muss zuallererst die Risikokultur verbessert werden. Dann können Datenbestände aufgebaut werden, mit dem Ziel, Risiken frühzeitig zu erkennen [DGR(2008), vgl. S.15ff].

[12] `https://de.wikipedia.org/wiki/Dienstleistungsqualität` (20.10.2015)

- Die Limits der Quantifizierung werden auch bei [McNeil et al.(2015)McNeil, Frey, and Embrechts, vgl. S.29-30] durch einen unangebrachten Gebrauch an komplexen mathematisch-statistischen Methoden und der Natur quantitativer Regulierung angesehen. Denn der erste Punkt führt dazu, dass das Topmanagement oder Aufsichtsorgane immer schwerer ermitteln können, wie viel Risiko denn nun im Unternehmen wirklich genommen wird. Der zweite Punkt führt zu einem übermäßigen Selbstvertrauen und blinden Vertrauen in Kennzahlen. Die historische Betrachtung als Teil von Kennzahlen (z.B. VaR Modellen) stellt dabei eine weitere Schwäche dar, denn man kann keine sichere Zukunft daraus ableiten. Das ist umso wahrer, als dass die VaR Quantifizierung von Risikoarten wie den OpRisk nur limitiert messbar ist [McNeil et al.(2015)McNeil, Frey, and Embrechts, S.29].

- Auch die Finanzinstitute setzen sich kritisch mit den Annahmen und Limitierungen der Risikoquantifizierung auseinander [MaRisk(2014), S. 247 bis 255]. Denn gerade in der Finanzindustrie musste während der verschiedenen Basler Akkorde massiv in Quantifizierung und Datenaufbereitung investiert werden und die Ergebnisse sind zwiegespalten. Risikoquantifizierungen haben gewichtige Schuld an manchen Krisen, z.B. die portfolio-insurance 1987, VaR 1998 oder die gaussian-copula 2008 [13].

- Laut einer groß angelegten Studie unter deutschen Firmen aus dem Mittelstand nutzen 87 % qualitative und 80 % quantitative Bewertungsmethoden. Besonders hervorzuheben ist, dass vor allem 30% der Familienunternehmen nur sehr schlichte Bewertungen durchführen, z.B. ohne Ausmaß und Häufigkeit separat zu bewerten [bdi and pwc(2011), S. 20]. Im Vergleich dazu nutzen nur 15% aller befragten Unternehmen so schlichte Methoden.

Das Risikomaß value-at-risk

Der value-at-risk (kurz VaR) ermittelt sich durch die Wahl einer Verteilungsfunktion, Betrachtungsperiode und eines Konfidenzniveaus (Alpha zwischen 0 und 1). Der VaR ist dann umgangssprachlich der kleinste Wert, an dem die Verteilungsfunktion das Konfidenzniveau erreicht oder erstmals überspringt [Damodaran(2008), vgl. Chp.7]. Es gibt keine einheitliche Berechnung des VaR, eine Übersicht als Entscheidungsbaum ist in Abbildung 3.12 abgebildet.

Die Limitierungen des VaR müssen ausdrücklich erwähnt werden:

- Das VaR wurde für die Verwendung bei Finanzprodukten von Banken entwickelt. Sie haben einen Haltebereich von 10, 30 oder ganz grob 90 Tagen und sind durch Derivate innerhalb kürzester Zeit vollständig absicherbar. Für diese Verwendung erscheint der VaR sinnvoll und die gelieferte Prognosegüte ist weithin akzeptiert. In der Industrie jedoch dominieren die operativen Risiken bei weitem gegenüber den Finanzrisiken. Die Oprisk sind meist nur über längere Zeiträume mess- und steuerbar. 12 Monatsprognosen sind für Oprisk knapp bemessen. VaR ist für das operative Geschäft daher

[13] `http://hbr.org/2011/11/can-risk-managers-manage-risk`(24.2.2014)

nicht brauchbar und Modelle die sich an den Jahresbericht koppeln, z.B. cashflow-at-risk oder EBIT-at-risk sind zu bevorzugen [Romeike and Hager(2009b), S.231ff].

- Nach [Damodaran(2008), vgl S.152ff] sind Limitierungen unbedingt zu beachten, denn das VaR wurde ursprünglich für das enge Feld der Marktrisiken entwickelt: Einige Risikofaktoren könnten gar nicht oder sogar doppelt einberechnet werden. Nicht normalverteilte Risiken können nicht mit VaR berechnet werden. Historische Daten können nicht automatisch die Zukunft vorhersagen. Nicht alle Korrelationen verhalten sich stationär über die Zeit.

- "Garbage in, garbage out" ist ein gängiges Zitat im Risikomanagement und soll auf die oft mangelnde oder nicht verfügbare Datenquantität und Datenqualität anspielen.

- Für einige seltene Risiken gibt es sogenannte fat-tails, jene Flächen die nach dem 95%- oder 99,9%-Quantil (Konfidenzniveau und Alphawert) übrig bleiben. Diese werden durch Verwendung des VaR ignoriert. Fat-tails sind Extremwerte, wie sie beispielsweise durch rund 2.150 dänische Feuerschadensfälle in [McNeil et al.(2015)McNeil, Frey, and Embrechts, S.151] analysiert wurden. Dieses Beispiel ist ein gängiger Beweis, dass die sogenannten fat-tails in Risiko Verteilungsfunktionen weitestgehend unterschätzt werden. Denn ein Konfidenzniveau von 99,9 % bedeutet umgangssprachlich nur ein Fall in tausend Jahren. Die Daten bei der dänischen Feuerwehr zeigen, dass mehr unerwartete und extreme Feuerschäden in diesem Zeitraum anfallen!

- Durch die unterschiedlichen Kerngeschäfte, ist die Marktpreisverschiebung bei Nichtfinanzfirmen im Vordergrund und die Marktwertveränderung bei Finanzfirmen. Der VaR ist daher für Nichtfinanzfirmen kaum geeignet [Bacher(2004), vgl. S.249ff]. Die Anwendung von VaR in Industrieunternehmen wird nach [Bacher(2004), vgl. S.118ff und 170ff] nur in finanznahen Aufgaben als sinnvoll erachtet, beispielsweise betriebliches Treasury, Handelsgeschäfte, Derivate, Beteiligungsmanagement, Commodity-Preisrisiken, Kredite, operationelle Risiken und Investitionen.

Zusammenfassend folgende Empfehlungen für die Verwendung des VaR:

- Als Instrument ist es gut für Marktrisiken wie Rohstoffschwankungen, Preisschwankungen, Aktienkurse, Währungskurse oder Zinsen geeignet [Diederichs(2012), S.107]. Bei anderen Risikokategorien stößt der VaR möglicherweise wegen Datenmangel und Verteilungsunkenntnis an seine Grenzen. Aufgrund seiner missbräuchlichen und unqualifizierten Anwendung ist der VaR in einigen Kreisen verrufen [Pergler(Oktober 2013), S.10]. Die Berechnung des VaR kann mit verschiedenen Methoden erfolgen, siehe Abbildung 3.12.

- Um die beträchtlichen Einschränkungen der VaR Methode bei einer unternehmensweiten Risikosteuerung zu überwinden, werden dafür expected-shortfall, cashflow-at-risk und earning-at-risk empfohlen [Diederichs(2012), S.107 und 117]. Beispiele eines cashflow-at-risk oder EBIT-at-risk im Einkauf und Verkauf werden bei [Romeike and Hager(2009b), S.231ff] behandelt.

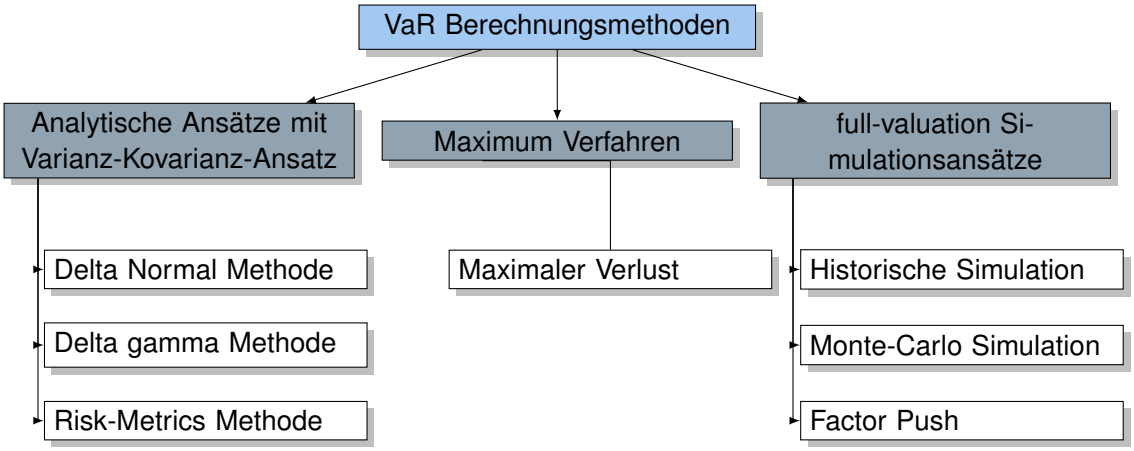


Abbildung 3.12: VaR Bewertungsmethoden nach [Romeike and Hager(2013), Abb. 3.13]

- Der expected-shortfall (ES) ist die durchschnittliche Überschreitung des VaR zum Konfidenzniveau von 95%- oder 99,9%-Quantil der gewählten Verteilungsfunktion. Damit erhält man beim Einsatz des ES auf jeden Fall einen höheren potenziellen Risikowert [Romeike and Hager(2013), S.119-120] .

Aggregierung der quantifizierten Risiken als Bestandteil der Analyse

Die Aggregation beschäftigt sich mit den Interdependenzen bzw. Korrelationen zwischen verschiedenen Risiken und der Ermittlung von Gesamtrisiken nach Risikokategorie, Unternehmensbereich oder anderen Dimensionen [Denk(2008), vgl. S.118].

Vorstufen der Aggregierung können semantisch wörtliche Beschreibungen oder (semi-) qualitative Risikomatrizen, Rankings- und Scoring-Verfahren sein [DGR(2008), vgl. S.215-218]. Quantitative Verfahren sind nach [DGR(2008), vgl. S.219ff] etwa eine Addition von Schadenswerten, VaR-Verfahren, Copulas (als Ansatz zur Aggregation verschiedener Risikokategorien) oder eine Neubewertung auf höherer Ebene.

Die Aggregierung ist Forschungsgegenstand des Risikomanagments und als solche gibt es interessante künftige Entwicklungen [DGR(2008), vgl. S.228ff]:

- Die industrieübliche best-practise bildet sich nur langsam heraus.
- Es gibt signifikante Branchenunterschiede im Nichtfinanzbereich.
- VaR Verfahren aus der Finanzindustrie kommen im Nichtfinanzbereich zum Einsatz und stehen unter Kritik, siehe Abschnitt 3.7.
- Auch praktische Rendite-Risiko Betrachtungen aus der operativen Unternehmenssteuerung sind denkbar.

- Korrelationen können nicht geschätzt werden und sind schwer zu ermitteln [DGR(2008), vgl. S.226].
- Im operationellen und strategischen Bereich gibt es im Nichtfinanzbereich besonders viele low-frequency-high-impact Risiken (schwarze Schwäne) und diese lassen sich nicht als Normalverteilungen im VaR darstellen [DGR(2008), vgl. S.223].

Da die Aggregation für die Einführung eines mittelständischen Risikomanagements bereits mit Risikolandkarten und Expertenschätzungen an die Leistungsgrenze stößt, wird in dieser Arbeit nicht detailliert darauf eingegangen. Es ist ein Anknüpfungspunkt für künftige Arbeiten.

3.8 Risikosteuerung

Zusammenfassung der Risikosteuerung :

$Das\ ist$ Die Steuerungsmaßnahmen sollen ein dem Risikoappetit des Unternehmens entsprechendes und ertragbares Restrisiko erzeugen [COSO(2006), vgl. S.104]. Es gilt dabei gut informierte und bewusste Geschäftsentscheidungen im Unternehmensalltag einzugehen.

$Grundlage$ Die in der Analyse bewerteten Risiken sollen unter Einbezug der Risikostrategie und Risikotragfähigkeit gesteuert werden [Denk(2008), vgl. S.127-128]. Siehe Abschnitt 3.7.

$Kriterium\ 1$ Welche Risiken lösen unmittelbaren Handlungsbedarf aus? Die Prioritäten müssen verteilt werden [Denk(2008), vgl. S.127].

$Kriterium\ 2$ Es gilt die Interdependenzen zwischen vielen Risiken und vielen Maßnahmen zu beachten. Die Risikoaggregation im vorigen Kapitel gibt zwar zusammengefasste Ergebnisse von Risikokategorien oder Unternehmensbereichen aber bei deren Risikobehandlung gilt es auch Interdependenzen der Maßnahmen zu bedenken. Im schlimmsten Fall können durch Maßnahmen des Risiko A sogar neue Risiken B entstehen [Denk(2008), vgl. S.128]! Eine Sichtweise des Gesamtrisikos mittels Portfolio (z.B. als Risikolandkarte) ist unabdingbar [Denk(2008), vgl. S.128].

$Kriterium\ 3$ Situationsbezogene Auswahl von aktiven und passiven Maßnahmen, jene die die Risikostruktur im Unternehmen verändern und jene die alles belassen wie es ist, indem sie z.B. versichern [Denk(2008), vgl. S.128].

$Kriterium\ 4$ Weitere Unterteilungen sind präventive, korrektive oder krisenbedingte Maßnahmen. Bei den präventiven Maßnahmen bedarf es eine ausgeprägte Risikokultur im Unternehmen. Die besten präventiven Maßnahmen erwecken den Anschein alles sei in Ordnung denn sie sind eine proaktive Risikobewältigung. Es hat den Anschein nirgendwo gäbe es Probleme und daher könnten sie bei schlecht ausgeprägten Risikokulturen Einsparungen zum Opfer fallen. Korrektive Maßnahmen sind passive Risikobewältigungen durch z.B. Risikotranfer oder -vorsorge und bedürfen keine Änderung

der Risikostrukturen. Bei krisenbedingten Maßnahmen bleibt die Risikostruktur unverändert und erst bei Materialisierung des Risikos wird gehandelt [Denk(2008), vgl. S.128].

$Ziel++$ Durch die Risikosteuerung soll eine Optimierung zwischen Ertragschancen und Verlustgefahren im Unternehmen erreicht und Fahrlässigkeit vermieden werden [Denk(2008), vgl. S.128].

$Ziel+$ Für die vielfältigen Risiken und Chancen braucht es mehr, als die immer gleichen Methoden. Man muss einen vielfältigen Methodenkasten zur Risikosteuerung im Unternehmen aufbauen, siehe Tabelle 3.6.

$Ziel+$ Eine effiziente Priorisierung und Steuerung im Risikomanagement spart Kosten und realisiert Chancen!

$Nachfolge$ Das Kapitel Abschnitt 3.9 zeigt die Kontrolle von Risiken durch passende Richtlinien, Kontrollaktivitäten und Überwachung. Mit Überwachung ist die der Informationssysteme, Maßnahmenpläne und des gesamten Risikomanagementprozesses gemeint .

Ansätze zur Risikosteuerung

Verschiedene Ansätze können in der Risikosteuerung benutzt werden:

- Die **Risikolimitierung** will mittels Messung und Kennzahlen die Risikosituation steuern und bereits während der Planungsphase Risikoübernahmen begrenzen. Bei der Begrenzung in der Planungsphase sollen die Risikorichtwerte (Risikokapazität) nicht überschritten werden, siehe Abbildung 3.1 [Denk(2008), vgl. S.130ff]. Diese Methode kann auch zur Kontrolle herangezogen werden.

- Die Risikobewältigung kann unterteilt nach Risikokategorien erfolgen, wie in [Gleissner(2011), vgl. S.200-213] und [Diederichs(2012), vgl. S.130-134] geschildert, siehe Tabelle 3.6.

- **Mittels Projektmanagementzugang** kann die Steuerung erfolgen, als Steuerung von vielen Einzelprojekten die das Risiko betreffen und wiederholende Folgeprojekte haben, siehe Tabelle 3.5.

- Ein Ansatz der Risikosteuerung ist das **ALARP Prinzip**, dabei wird das Restrisiko nach Umsetzung der Maßnahmen nach Sinnhaftigkeit und gesellschaftlicher Tragfähigkeit bewertet (engl. residual risk), siehe Abschnitt 2.5.

- **Standardisierte Maßnahmen** die in Maßnahmenkategorien unterteil sind und einfach anpassbar verwendet werden können, sind eine einfache Möglichkeit der Risikobewältigung. In einem Maßnahmenplan (auch Maßnahmenkatalog genannt) werden alle für ein Risiko bestimmten und darauf angepassten Maßnahmen eingetragen und deren Umsetzungsstatus überwacht [ISO(2009), S. 29].

- **Frühindikatoren** nach [Denk(2008), vgl. S.133] sind ein Sonderfall der Kennzahlen Methode. Dabei geht es bei Frühindikatoren um jene Messungen, die bereits Ereignisse ankündigen bevor diese eintreten. Diese Methode ist insofern aufwendig, als dass zum jeweiligen Risiko passende und messbare Faktoren gefunden werden müssen, beides stellt sich in der Praxis als schwierig heraus. Beispiele für Frühindikatoren sind Vorbeben für Erdbeben oder Schwingungen bei der Wälzlagerüberwachung die ein Versagen ankündigen (sogenannte CREST Werte [14].) oder Verschiebungen von Zahlungszielen die Zahlungsschwierigkeiten ankündigen. Siehe Abschnitt 3.8.

Methoden zur Risikosteuerung

- Die **Detailuntersuchung** ist als Maßnahme für einschlägige und komplexe Risiken gedacht, etwa der EDV, Bausubstanz, Marktumfeld, etc. Dabei darf es keine mehrmalige Methode sein, sondern eine einmalige, projektgesteuerte Untersuchung mit Zielen, Ressourcen und Zeitplan.

- Risiko **vermeiden** durch z.B. Geschäftsfeldeinstellung, Outsourcing einzelner Komponenten oder Tätigkeiten, etc.

- Risiko **reduzieren durch abnehmende Bedeutung** z.B. Redundanz, Reaktionszeit.

- Risiko **reduzieren durch abnehmende Häufigkeit** z.B. durch oftmaligere Wartung sinkt die Ausfallwahrscheinlichkeit.

- Das Risiko kann auch **geteilt** werden, z.B. durch Versicherung, Hedging, Pönalen, etc.. Ob Hedging oder Versicherungen für die jeweilige Unternehmensbranche und den jeweiligen Führungsstil relevant sind, muss untersucht werden [Damodaran(2008), S. 302]. Damodaran unterteilt die Vorteilhaftigkeit eines Hedging nach Kategorien und beurteilt dabei ob die Firma: Marktbarrieren hat, Höhe des Fremdkapitalhebels, ob man diversifizierte oder nicht diversifizierte Geschäftsfelder hat und schließlich ob man markt- oder firmenspezifische Risiken hat.

- Die Maßnahme das **Risiko zu tragen** bzw. es schlicht zu akzeptieren, darf erst nach ausgiebiger Analyse innerhalb des Risikomanagementprozesses fallen.

- Eine Maßnahme kann auch außernatürliche und häufigere **Sonderkontrolle** sein.

- Eine **Überwachung durch automatisierte Kennzahlen** in Form eines Frühwarnsystems (siehe Tabelle 3.7) ist ebenfalls eine passende Maßnahme für kritische und nicht branchenimmanente Risiken.

- Für gewisse seltenere Risiken (engl. black-swans) ist eine der passenden Maßnahmen ein **Krisenmanagement** vorzubereiten. Dabei sind insbesondere seltene höhere Gewalten oder brancheninhärente Risiken gemeint. Eine **Behandlung von De-**

[14] https://infosys.beckhoff.com/index.php?content=../content/1031/tf3600_tc3_condition_monitoring/1162493835.html&id=(26.10.2015)

sasterfällen [Denk(2008), vgl. S.126] muss für die brancheninhärenten Risiken vorbereitet werden, um schnelle Handlung zu garantieren. Der Vorstandsvorsitzende z.B. einer Fluglinie hat diverse Katastrophenmanagement Pläne ausgearbeitet, eines beinhaltet ein Paket mit weißem Hemd, schwarzer Krawatte und einer Trauerrede um bei Flugzeugabstürzen schnell öffentlich Auftreten zu können. Eine weitere Maßnahme für seltene Risiken kann als s.g. Force Majeure Klauseln in Geschäftsverträgen eingearbeitet werden.

Alle Risiken sollten regelmäßig z.B. einmal im Jahr die Risikobewertung neu durchlaufen. Risikoexperten oder Risikokomitees können zusätzlich Sonderkontrollen vordern. Es ist wichtig auch regelmäßig die Maßnahmen in Frage zu stellen. Es kann sich mit der Zeit ändern, ob ein bestimmtes Risiko nun besser nicht mehr oder wieder versichert bzw. gehedged werden sollte! Die Abbildung 3.13 zeigt den Entscheidungsprozess zur Auswahl der zum Risiko passenden Risikosteuerung Methode.

Die Risikosteuerung kann grob in zwei Kategorien unterteilt werden. Die der Risikovermeidung durch passive Methoden wie Versicherung, Hedging oder Vermeidung, welche die Risikostruktur nicht verändern. Und jene aktiven Methoden, wie Reduzierung, Kontrollen oder Akzeptierung, die in den Unternehmensalltag die Risikostruktur eingreifen und überall ein Risikomanagement installieren [Damodaran(2008), S. 301ff] und [Denk(2008), vgl. S.128]. Eine grobe Gegenüberstellung beider Zugänge sind in Abbildung 3.13 dargestellt.

Ein Teilgebiet der Risikosteuerung ist ein Projektmanagement bzw. Projektsteuerung über die offenen Maßnahmen und anderen Bestandteilen der Risikomanagementkomponenten. Der Maßnahmenplan soll folgende Komponenten beinhalten [ISO(2009), vgl. Kp. 5.5.2 und 5.5.3]:

- Eine Übersicht der Prioritäten,
- Begründung der Auswahl,
- Teilschritte zur Bewältigung,
- Ressourcenbedarf,
- Leistungsmessung,
- Verantwortlichkeiten,
- Anforderungen an Überwachung,
- Zwischenstände und
- Terminpläne.

Umsetzungsbeispiele eines Maßnahmenplans finden sich in Tabelle 3.5 und Abschnitt 4.5.

Zur Bewältigung der vielfältigen Risiken, beim gleichzeitigen Mitnehmen der Chancen, bedarf es einen ebenso vielfältigen Methodenkasten der Risikosteuerung, wie in Tabelle 3.6 lückenhaft gezeigt.

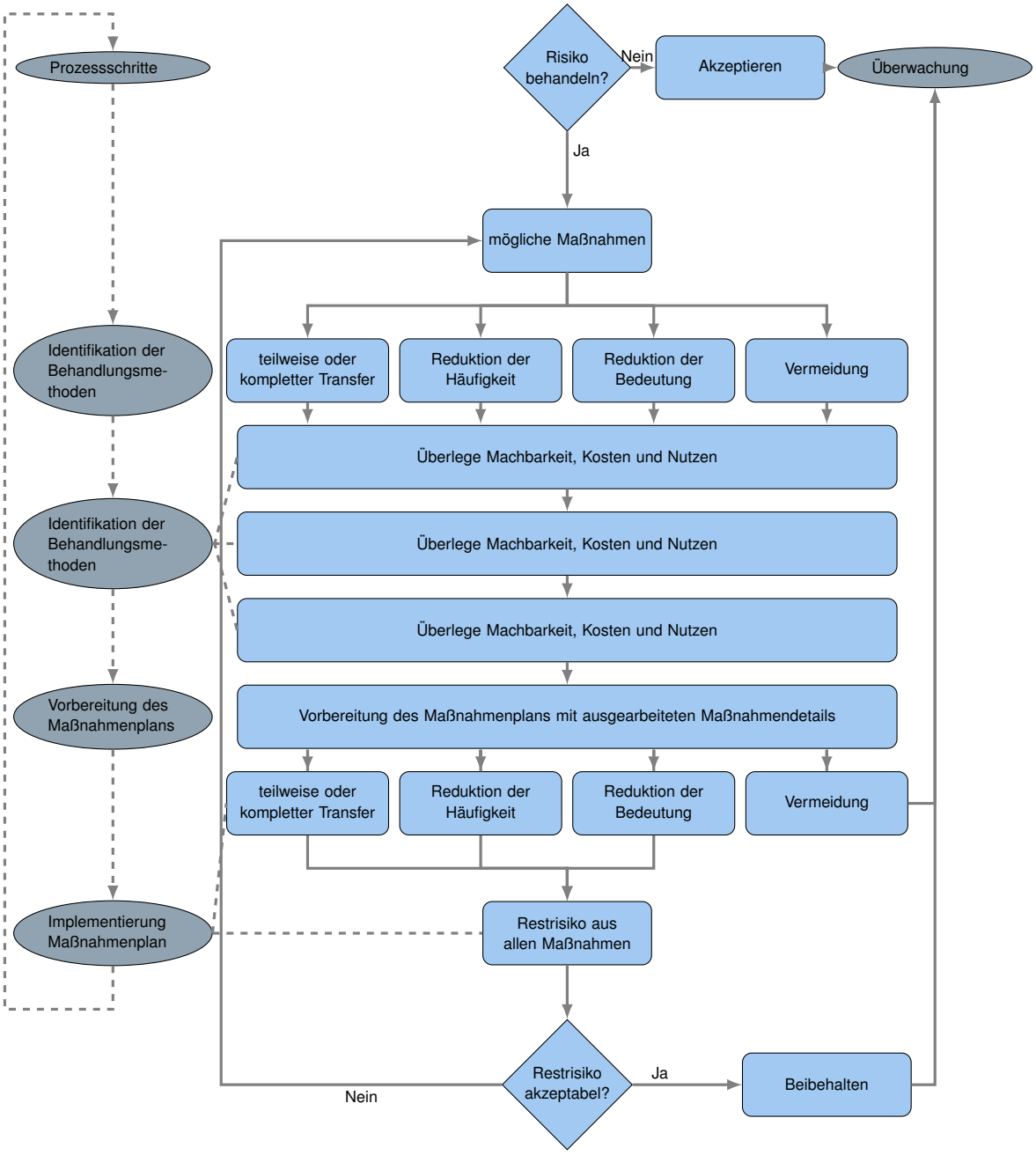


Abbildung 3.13: Entscheidungsprozess zur Auswahl einer zum Risiko passenden Risikosteuerungsmethode [Popescu(2014), F.19]

ID	Name d. Risiko	IST Risiko	PLAN Risiko	Maßnahme	Nicht gestartet	Planung	Approved	in Arbeit	Fertig	KPI Status	Priorität	Termin TTMMJJ	Verantwortlich	Kosten in TEUR
Risikoinfo				Status Maßnahmen							Organisation			
23	Umsetzung Strategie fehlerhaft	5	2	verringern					●	◔	4	01 11 15	MM	50
15	Betriebs-unfall	3	2	versichern		●				NA	4	NA	JG	NA
28	Schlechte Invest-ments	4	3	verringern				○		◔	3	N 15 04 15	CA	NA
3	Fehler Lieferket-te	3	2	Transfer				◐		◔	2	NA	MM	25
44	CO2 Re-gulierung	2	1	Lobby		●				NA	3	30 10 15	BW	25

Tabelle 3.5: Beispielhafte Umsetzung eines Risikomanagementplans [Popescu(2014), F. 21]

Viele der möglichen Steuerungsinstrumente sind in Unternehmen bereits vorhanden und im Einsatz. Die Aufgabe des Risikomanagements besteht kurzfristig darin, diese für einen vollständigen Risikomanagementprozess zu nutzen und zu überprüfen. Langfristig gehören Steuerungslücken geschlossen und die Methoden verbessert [Diederichs(2012), vgl. S. 134].

Früherkennung

Mit Hilfe von Früherkennungssystemen sollen Risiken so weit wie möglich vor ihrem Eintritt erkannt werden, um dem Unternehmen Zeit zu geben, im normalen Betrieb mit Maßnahmen gegenzusteuern [Diederichs(2012), S. 74]. Früherkennungsindikatoren brauchen Kennzahlen (ähnlich der KPI) die Aufgrund messbarer Informationen innerhalb eines Informationssystems generiert werden können [Denk(2008), S.94]. Die wesentliche Schwäche von Kennzahlen- und hochrechnungsorientierten Frühwarnsystemen besteht in dem vorhandenen Datenmaterial, das oft nur vergangenheitsbezogen ist [Diederichs(2012), S. 75 und 78]. Es reicht nicht, gewisse interne Daten monatlich händisch einzupflegen und auch nicht, nur mittels externer Daten zu arbeiten. Unternehmen die ein Frühwarnsystem aufbauen wollen, müssen ihre Informationssysteme und internen Daten aufwendig dafür auslegen!

Leistungswirtschaftliche Risiken	Finanzwirtschaftliche Risiken	Risiken aus Management und Organisation	Externe Risiken
Beschaffung Ausweichlieferanten Lieferantenaudits Einkaufsrichtlinie	**Kapitalbeschaffung** Forderungsverkäufe Fondsbildung als interne Deckungskonzepte	**Management** Schulungen Integritätsmanagement Führungsgrundsätze	**Markt- und Kundenrisiken** Geschäftsbedingungen Haftungsausschüsse Bonitätsprüfungen
Leistungserstellung Ausweichanlagen Prozesskontrollen Betriebsunterbrechung Versicherung	**Kapitalanlage** Investitionsrichtlinie Beteiligungscontrolling Due Dilligence	**Organisationsstruktur** Geschäftsordnung Stellenbeschreibung Genehmigungsregelungen	**Gesetzgebung** Verbandsarbeit Schulungen Recherchen
Logistik Warenwirtschaftssystem Vertragsgestaltungen Transportversicherung	**Liquidität** Finanzierungsrichtlinie Cash Pooling Kreditversicherung	**Personal** Nachwuchsförderung Personalentwicklung Coaching	**Natürliche Umwelt** Umweltschutzrichtlinien Brandschutz Standortwahl
Absatz Kundenverträge Kundenbefragung Preisgestaltungen	**Währungen** Hedging Devisentermingeschäfte Währungsderivate	**Forschung und Entwicklung** Vorschlagswesen Innovationsanalyse Patentierung	**Soziokultur** Trendforschung Ethische Regeln Mitarbeiterschulungen
Marketing Imagekampagne Kundenbindungssystem Trendscouts	**Zinsen** Fristenkongruente-Finanzierungsstruktur Zinsderivate	**IT** Vorschlagswesen Innovationsanalyse Benchmarking	**..... u.v.m** .... etc.

Tabelle 3.6: Beispielhafte Einteilung der Steuerungsmaßnahmen nach Risikokategorie [Diederichs(2012), Abb. 3-56]

Die Kennzahlen eines Frühwarnsystems brauchen keinen gegenseitigen Zusammenhang wie in einem Kennzahlensystem, sie sind nur eine Liste die je nach Bedarf für die Risikosteuerung des Unternehmens angepasst werden kann [Scheld(2012), Kp. 3.1.2.5].

Eine weitere Schwierigkeit ist die Natur von schwachen Signalen bzw. Früherkennungssignalen als Informationen mit unklarer Herkunft und Auswirkung. Meistens sind es unbestimmte und unsichere Vermutungen über künftige Umfeldveränderungen. Daher ist es wichtig, ein Frühwarnsystem unkompliziert aufzubauen, denn die Einfachheit erleichtert die Übersicht über die Zusammenhänge und Kommunikation [Scheld(2012), Kp. 3.1.2.5].

Hervorzuheben ist, dass neben der kontinuierlichen Verbesserung der Risikokultur, vor allem das Frühwarnsystem plus vorgeplanten Krisenmanagement den größten Nutzen eines Risikomanagementsystems darstellt. Die Frühwarnung ist nur bei fortgeschrittenem Reifegrad im Risikomanagement möglich, dieses Ziel sollte man jedoch nicht aus den Augen verlieren, denn erst durch Frühwarnung entfaltet das Risikomanagement sein volles Potential! Erfolgreiche Früherkennung muss simpel genug (engl. simplicity), selektiv bei den Methoden (engl. selectivity) und im Prozess transparent sein [Plaschke et al.(2013)Plaschke, Rodt, Pidun, and Günther, Exhibit 3.] [15].

Der Aufbau eines indikatorgetriebenen Frühwarnsystems erfolgt nach [Diederichs(2012), vgl. S. 79] in 5 Schritten:

1. Ermittlung der Beobachtungsbereiche für die Früherkennung von relevanten Risiken und Chancen.
2. Auswahl der passenden Indikatoren bzw. Kennzahlen, dies kann nach Eindeutigkeit, Vollständigkeit, rechtzeitiger Verfügbarkeit oder ökonomischer Vertretbarkeit erfolgen.
3. Pro Indikator muss ein kritischer Sollwert, der eine Benachrichtigung auslöst, definiert werden und ein sinnvoller Toleranzbereich.
4. Festlegung eines Beobachtungs- und Berichterstattungsprozesses.
5. Aufbau einer Informationsverarbeitungsstelle zur Aufnahme und Analyse der Signale und Generierung der Warnsignale für vordefinierte Empfänger!

Der Aufbau eines strategischen Frühwarnsystems ist nach [Diederichs(2012), vgl. S. 80] möglich, darauf wird hier nicht näher eingegangen.

In der Praxis haben sich einzelne Institute und Firmen in den letzten Jahren hervorgetan, indem sie auf regelmäßiger Basis hochwertige Kennzahlen aktualisieren oder den aktuellen Wissensstand veröffentlichen, siehe Abschnitt 2.3. Dies kann als erster Hinweis zur Informationsgewinnung dienen. Auch Ratings können in die Frühwarnsysteme eingebaut werden [Gleissner(2011), vgl. S.286].

[15] `https://www.bcgperspectives.com/content/articles/financial_management_art_of_risk_management/` (24.10.2015)

Fortgeschrittene Unternehmen können bei der Konzeption ihres Frühwarnsystems auf Arbeiten von [Ansoff(1975a), S.21-33] aufbauen. Dessen Theorie des strategischen Frühwarnsystems erklärt, dass bevor Toprisiken (höhere Gewalt, Markt-, oder Technologieveränderungen, etc) stattfinden, schwache Signale in Form von Trends oder Medienberichten messbar wären. Der dazugehörige Prozess ist für fortgeschrittene Risikomanagement Reifegrade gedacht.

In Tabelle 4.8 sind Beispiele für Früherkennungsindikatoren. Quellen finden sich einige, so z.B. [MaRisk(2014), Abb. 53], der key-risk-indicator bei der Europäischen Bankenaufsicht (EBA) [16], oder die hier aufgelisteten allgemein verwendbaren Frühindikatoren nach [Diederichs(2012), S. 77]:

3.9 Risikokontrolle

In der Einleitung zu Abschnitt 3.5 ist bereits erwähnt, dass bei den Kontrollaktivitäten keine saubere Unterscheidung zwischen COSO und ISO möglich ist, denn COSO II hat die zwei Komponenten Kontrollaktivität und Überwachung. ISO 31000 hat jeweils eine Überprüfung im Risikomanagementprozess und -rahmen. In dieser Arbeit versteht sich die Kontrolle als Schritt im Demingregelkreis und 2. line-of-defense. Die Überwachung (siehe Abschnitt 3.11) ist die unabhängige und alles überblickende 3. line-of-defense.

Zusammenfassung der Risikokontrolle wie sie in dieser Arbeit verstanden wird:

Das ist Eine unabhängige Kontrolle der Informationssysteme, gesteuerten Maßnahmenpläne und des gesamten Risikomanagementsystems. Sie dient innerhalb des Demingregelkreises der ständigen Verbesserung des operativen Risikomanagement der 1. line-of-defense. Meist wird die Kontrolle innerhalb der 2. line-of-defense organisiert und soll mit Experten, Befugnissen und Ressourcen dermaßen ausgestattet sein, dass eine zeitnahe, unabhängige und kritische Bewertung auf allen Unternehmensebenen möglich ist [COSO(2006), vgl. S. 61ff] .

Grundlage Die Risikosteuerung setzt Maßnahmen damit Risiken im Griff gehalten werden. Dabei kontrolliert die Risikosteuerung ähnlich einem Projektmanagement die Umsetzung der Maßnahmen und kann als Maßnahme Sonderkontrollen einsetzen, siehe Abschnitt 3.8.

Kriterium 1 Eine Einbindung in die Risikobeurteilung ist laut [Bungartz(2012), vgl. S. 73] und Einbindung in die Risikosteuerung laut [COSO(2006), vgl. S. 61ff] vorteilhaft. Bei Coso steht der Gedanke im Vordergrund, dass die in der Steuerung definierten Maßnahmen auch kontrolliert werden müssen und bei Bungartz ist die Ausstattung mit Informationen entscheidend. Die Beurteilung welcher der beiden Zugänge besser ist oder ob beide nötig sind, wird in dieser Arbeit nicht ermittelt. Es ist wichtig, dass dies in Form von Vorschriften und Verfahren z.B. in einem Organisationshandbuch passiert [Bungartz(2012), vgl. S. 73] .

[16] `http://www.eba.europa.eu/risk-analysis-and-data/risk-dashboard` (24.10.2015)

interne oder externe Risiken	Indikatoren
Externe Bereiche: Gesamtwirtschaft bzw. Makroökonomie	Zinsen, Wechselkurse, Inflationsraten, industrielle Nettoproduktion, Tariflohnniveau, Außenhandel, Geldvolumen, Konjukturindizes, Geschäftsklima, Investitionstendenzen, Marktwachstum
Gesellschaft und Kultur	Bevölkerungswachstum, Bevölkerungsstruktur, Arbeitslosenzahl, Zahl offener Stellen, Gewerkschaftsforderungen, Konsumneigung, Einkommensentwicklung, Bildungsstand, Lebensstil, Wertvorstellungen, Wanderungsbewegungen, Haushaltsgröße
Technologie	Innovationen, Werkstoffentwicklung, Unterbrechung technologischer Trendlinien, Veränderungstendenzen der Produktions- und Verfahrenstechnologien bei Wettbewerbern und Forschungsinstitutionen
Politik und Recht	Systemstabilität, politische Krisen, Parteienverhältnisse, Regierungswechsel, Gesetzesvorbereitungen und -vorlagen, Rechtssicherheit, politische Organisationen, Außen- und Innenpolitische Ereignisse, Außen- und Innenpolitische Tendenzen
Ökologie	Umweltverträglichkeit der Produkte, Produktionsverfahren und Einsatzstoffe, Volumina bekannter Rohstoffvorkommen
Interne Bereiche: Forschung und Entwicklung	Entwicklungskosten, Patentmeldungen, Patentverletzungen, Teilevielfalt
Beschaffung	Marktpreise, Beschaffungskonditionen, Qualitätsniveau der Güter, Angebotsvolumen im Markt, Termin- und Lieferantentreue, Warenumschlag
Produktion	durchschnittlicher Jahresverbrauch je Rohstoff, Ausstoßhochrechnung, Instandhaltungskosten, Altersstruktur und Technologiestand des Maschinenparks, Auslastung, Lagerbestände, Materialausnutzung, Ausfallquote und Wartungsgrad des Maschinenparks, Fehlerhäufigkeit
Absatz	Auftragseingänge je Produkt und Land, Auftragsbestand, Umsatzhochrechnung, Nachfragevolumina Topkunden, Programmbreite, Preise, Marktanteil, Erfolgsgrad der Kundenakquise, Veränderungen bei Eigentümerstruktur, Todesfälle, Verfahren von Kunden, Negative Schlagzeilen, Verlust Schlüsselkunden, Vertragsverstöße
Marketing	Bestell- und Kaufverhalten der Kunden, Konsumentenstimmungen, Reklamationsraten, Preis- und Programmpolitik der Konkurrenz, Image der Eigenprodukte im Vergleich zur Konkurrenz
Personal	Fluktuationsraten, Krankenstände, Lohn- und Gehaltszuwächse im Konkurrenzvergleich, Herrschafts- und Exklusivwissen , Betriebsunfälle, Personalkosten
Finanzen	Entwicklung der Liquidität und Rentabilität, Wertschöpfung, Forderungsbestand, Ausnutzung von Zahlungszielen, Investitionsquote, Abschreibungen, Verschuldungsgrad
Informationstechnologie	Datenverluste, unberechtigte Zugriffe auf interne Daten, Verfügbarkeit, Sicherheit, Integrität

Tabelle 3.7: Beispielhafte Indikatoren und Frühindikatoren [Diederichs(2012), Abb. 3-19]

$Kriterium\ 2$ Die Umsetzung der Risikokontrolle muss auch organisatorisch und firmenspezifisch geklärt werden. Entscheidet ist, ob die Risikokontrolle zentral durch den Risikomanager alleine, dezentral oder durch andere Abteilungen wie beispielsweise die interne Kontrolle (IKS) oder interne Revision erfolgt. Dies kann komplett ausgelagert oder in Zusammenarbeit mit dem Risikomanagement erfolgen. Zwischen IKS und Risikokontrolle bestehen Ähnlichkeiten, daher können in diesem Schritt des Risikomanagementprozesses auch Methoden aus dem IKS herangezogen werden [COSO(2006), vgl. S. 66] und [Bungartz(2012), vgl. S. 53].

$Kriterium\ 3$ Die Kontrolle der Informationssysteme ist eine weitere wichtige Aufgabe der Kontrolle. Sie beinhaltet die Überprüfung des IT-Management, IT-Infrastruktur, Sicherheitsmanagement, Informationsverarbeitung, Softwarebeschaffung, -entwicklung und -wartung [COSO(2006), vgl. S. 66].

$Kriterium\ 4$ Die Risikokontrolle ist ein Schritt des vierteiligen Demingkreislaufs und muss als solcher eine Rückkopplung zu den anderen Schritten des Risikomanagementprozesses zulassen [Denk(2008), vgl. S.133ff], als ständige Verbesserung!

$Kriterium\ 5$ Die Auswahl und der Aufbau der Kontrolle muss an die Möglichkeiten des Unternehmens angepasst sein [Bungartz(2012), vgl. S. 73]. Dabei muss, wie bei allen betriebswirtschaftlichen Prozessen, bei der Kontrolle ein Gleichgewicht zwischen Kosten, Qualität und Zeit erzielt werden.

$Kriterium\ 6$ Eine schriftliche Dokumentation der Kontrolle ist gesetzlich gefordert und auch für die Weiterentwicklung des Unternehmens wichtig [Denk(2008), vgl. S.134]. Im Zuge der ordentlichen Geschäftsführung gehört das selbstverständlich dazu und als Beweislast im Falle von Katastrophen ist Dokumentation die entscheidende Entlastung.

$Ziel\ ++$ Die Kontrollmechanismen dienen als Mechanismus dem Erreichen der Unternehmensziele, in dem sie sicherstellen dass die Risikosteuerungsmaßnahmen und Managemententscheidungen eingehalten wurden [COSO(2006), vgl. S. 61-62]!

$Ziel\ +$ Wie bereits in der Erklärung eines IKS in Abschnitt 3.4 geschildert, sind die Hauptaufgaben der Kontrolle die Sicherheit, Wirtschaftlichkeit und Ordnungsmäßigkeit im Unternehmen zu gewährleisten.

$Nachfolge$ Die Überwachung und Überprüfung der Kontrolle als 2. line-of-defense durch die Überwachung als 3. line-of-defense. Dies kann je nach Unternehmen etwa durch das interne Kontrollsystem, interne Revision oder einem Gremium im Aufsichtsrat erfolgen, siehe Kapitel Abschnitt 3.4. Dabei sollen Schwächen in der Berichterstattung und der Kontrolltätigkeit in der 2.line-of-defense aufgezeigt werden und das Risikomanagementsystem unabhängig beurteilen.

Ansätze zur Risikokontrolle

Die Kontrolle kann nach verschiedenen Gesichtspunkten konzipiert werden, wobei die Unternehmensleitung entscheidet welche zum derzeitigen Unternehmen passen [Bungartz(2012), vgl. S. 60-62]:

- **Manuelle oder Automatische** (systembasierte) Kontrollaktivitäten, unterscheiden sich durch den Einsatzgrad an Software im IT-System.
- **Präventive** (vorbeugende) oder **detektive** (aufdeckende) Kontrollaktivitäten sind fast schon Philosophien und unterscheiden sich im Zeitpunkt in dem man den größten Teil der Kontrollarbeit leistet. Denn es braucht je nach Risiko sowieso beide Varianten. Präventive Kontrollen verhindern materialisierende Risiken, sind jedoch meist teurer und aufwendiger!
- **Primäre und Sekundäre** Kontrollaktivitäten haben einen unterschiedlichen Grad bei der Verminderung des Risikos. Wobei die primären Kontrollen (Schlüsselkontrollen) das Risiko entscheidend reduzieren und teils gesetzlich vorgeschrieben sind. Die Sekundären könnten durch Primäre ersetzt werden, haben jedoch oft den Vorteil dass sie beiläufig oder billiger zu unternehmen sind.
- Kontrollaktivitäten über **Routineprozesse oder über Nicht-Routineprozesse**, unterscheiden sich im Aufwand und ob man diese als Unternehmen lieber in den Alltag integriert oder separat abhält. Manche Kontrollen können auf Grund von z.B. technischen Gegebenheiten oder weil es sich um Toprisiken handelt nur außernatürlich abgehalten werden.
- Kontrollaktivitäten auf **Unternehmensebene** (-führung) oder auf **Prozessebene**, setzen an verschiedenen Hierarchiestufen im Unternehmen an, ähnlich dem top-down oder bottom-up Ansatz.
- Nach Kaplan gibt es 3 mögliche **Typen eines Kontrolleurs**, wobei trotz Regulierungsversuchen, keiner universal einsetzbar ist. Seine Annahmen betreffen dabei die Kontrolleure als Personen in einer unternehmerischen Umwelt. Diese können nicht alles wissen und das Kontrollieren stellt per se einen schmerzhaften und nicht natürlichen Vorgang da. Alle Typen haben vorteilhafte Einsatzgebiete und Nachteile [Kaplan and Mikes(06.2012), vgl. S. 6-8].
  - Interne oder externe, unabhängige Experten (engl. technical experts) können besonders bei hochspezialisierten Firmen, z.B. in der technischen Produktentwicklung, einen Projektmanagement Weg einschlagen. Bei diesen Firmen gibt es zwar hohe interne Risiken durch die Entwicklung, jedoch ändere sich die Natur der Risiken nicht.
  - Facilitators sind kleine zentrale, interne Expertengruppe die die Risikoeigner einbeziehen und in kleinen Schritten verändern. Diese können in Branchen mit stabilen Marktumfeld operieren, z.B. haben Energiekonzerne ein stabiles Technologie-

und Kundenverhalten. Dabei sind Risiken oft Interdependenzen oder die komplexe Organisationsstruktur, die sich oft über Jahre und verborgen aufbauen. Diese können in Workshops mit anonymus-voting und abschließenden Gruppen-Konsens erarbeitet werden.

– Embedded Experts findet man z.B. in der Finanzindustrie mit schnellen Marktveränderungen. Sie müssen das Risiko kontinuierlich beobachten, mit den Risikoeigner Seite an Seite arbeiten und das Risiko während der Entscheidungsfindung beeinflussen. Die größte Gefahr ist Verbrüderung der operativen und kontrollierenden Mitarbeiter (engl. go-native).

Methoden zur Risikokontrolle

- Ein **Risikoausschuss** kann permanent installiert werden, um zwischen den Befugnissen des Risikomanagers und der Geschäftsführung eine Entscheidungsebene zu haben oder auch als Kontrollgremium im Sinne der Überwachung in Abschnitt 3.11. Die Zusammensetzung der Gruppe sollte gut überlegt sein, auf jeden Fall sollte der Risikomanager darunter sein [Diederichs(2012), vgl. S. 143]. Gängige Aufgaben sind z.B. [Diederichs(2012), vgl. S. 145].

- **Kennzahlen** in der Form von regelmäßig oder automatisch aktualisierten Kennzahlen sind eine passende Form der Risikokontrolle [pwc(2008), S.19]. Da die Kennzahlen als Kontrolle dienen, können das auch Messergebnisse oder Berechnungen sein, die expost zur Verfügung stehen. Bei Coso wird diese Methode als top-level-review bezeichnet, in der die Unternehmensführung Soll- mit Ist-Werten vergleicht [COSO(2006), vgl. S. 62].
  Kennzahlen sind ebenfalls eine mögliche Form der Risikobewertung und -steuerung. Beispiele siehe Tabelle 3.7 oder Abschnitt 3.8.

- Eine ähnliche Methode ist die **Risikolimitierung** nach [Denk(2008), vgl. S.130]. Er beschränkt das Risiko durch Festsetzung von Limite auf Einzelgeschäft- und Gesamtunternehmensebene auf Basis von VaR oder Sensitivitätsanalysen. Nach [Kaplan and Mikes(06.2012), vgl. S.5] ist diese Limitierung bzw. negativformulierte Grenzsetzung eine effektive Art der Kontrolle. Diese können in einem Unternehmenskodex verfasst werden, ähnlich dem amerikanischen bill-of-rights Grundgesetz, in dem 9 von 10 Punkte eine negativformulierte Einschränkung sind. Diese Methode kann auch zur Beurteilung herangezogen werden.

- Ein effektives **Hinweissystem** (engl. whistle-blower-system) ist eine sehr wichtige Kontrolle [Kaplan and Mikes(06.2012), vgl. S.5]. Darunter zählt auch Anonymität und passende Prozesse zur Bewertung des Richtigkeitsgehalts!

- Eine **strenge Funktionstrennung** zwischen den Verpflichtungen und Kontrolleuren, wie sie im three-lines-of-defense Modell vorgeschlagen wird, trägt zu einer effektiven Kontrolle bei [Kaplan and Mikes(06.2012), vgl. S.5] und [COSO(2006), vgl. S. 63]!

- Die strenge Funktionstrennung widerspricht dem “funktionalen oder betrieblichen Management” als Kontrollmethode. Der verantwortliche Manager überprüft dabei selbst die Leistungsberichte und relevanten externen Berichte [COSO(2006), vgl. S. 62].
- Die wesentlichen **Faktoren eines Kontrollumfelds** sind laut [Bungartz(2012), vgl. S. 50ff]:
  - die Bedeutung von Integrität und ethischen Werten z.B. wie in Abschnitt 3.9, durch einen Verhaltens- und Ethikkodex im Unternehmen,
  - die Bedeutung der fachlichen Kompetenz im Unternehmen,
  - die Tätigkeit des Überwachungsorgans,
  - die Philosophie und das Geschäftsgebaren des Managements,
  - die Organisationsstruktur,
  - die Zuordnung von Weisungsrechten und Verantwortung sowie
  - die Grundsätze der Personalpolitik.
- **Physische Kontrollen** sind bei Anlagen, Vorräten oder Bargeld nötig. Diese können in Form von z.B. Audits erfolgen [COSO(2006), vgl. S. 63].
- **Programme zur Vermeidung doloser Handlungen**, etwa Bilanzfälschung, Betrug, Täuschung oder Unterschlagung [Bungartz(2012), vgl. S. 76].
- **Anwendungskontrollen** nach [Bungartz(2012), vgl. S. 64] können in modernen IT unterstützten Unternehmen eine passable proaktive Kontrollmethode sein:
  - Klassifikation von Daten von streng geheim, vertraulich, Management, Mitarbeiter bis öffentlich und einen logischen Zugriffsschutz mit Benutzer-ID und Passwort
  - Eingabe- bzw. Plausibilitätskontrollen z.B. durch Wertbereiche in Eingabefeldern mit min. und max. und Vorgabe bei Einheiten und Dimensionen.
  - Verarbeitungs- und Ausgabenkontrollen, die sicherstellen dass die Informationsverarbeitung fehlerfrei abläuft
  - Protokollierung und Schnittstellenprotokolle bei der Informationsverarbeitung
- The-levers-of-control-model (dt. **Kontrollhebel Modell**) nach [Simons(1999), vgl. S. 16ff], erklärt die Hebel der internen Kontrolle und verlangt, dass sie den Strategieprozess begleiten. Zusätzlich zum Modell erklärt [Simons(1999), vgl. S. 4ff] die drei internen Quellen von Risiken, nämlich das Unternehmenswachstum, die Unternehmenskultur und das Informationsmanagement. Diese wurden bereits in der Tabelle 3.1 verwendet, um die überschlägige Risikosituation im Unternehmen zu berechnen.
  Das Kontrollhebel Modell wurde primär für die interne Kontrolle entwickelt, aber auch für die Verwendung innerhalb der Kontrolle im Risikomanagmentprozess scheint es passabel. Die 5 Kontrollhebel haben einen Selbsttest mit folgenden Fragen:

- Belief-systems, also ob die Unternehmensführung die Unternehmenskultur und Ethik richtig kommuniziert? Der Erfolg zeigt sich, in dem die Mitarbeiter es auch annehmen und im Alltag anwenden.
- Boundary-systems bezeichnet die roten Linien in einem Unternehmen und ob die Unternehmensführung diese klar identifiziert hat? Dabei müssen diese Grenzen auch mit konkreten Beispielen wie Handlungen oder Benehmen definiert werden, die Konsequenzen auslösen.
- Funktionieren die diagnostic-control-systems so gut, dass sie kritische Leistungskennzahlen passend darstellen?
- Sind interactive-control-systems wirklich interaktiv ausgelegt und lernfähig?
- Wird die traditionelle interne Kontrolle mit genügend Budget ausgestattet um gute Arbeit leisten zu können?

Vorlage eines Verhaltens- und Ethikkodex als präventive Methode

Ein Kodex ist nur so gut, wie der im Unternehmen real gelebte tone-of-the-top, daher muss das Topmanagement den vorhandenen Kodex mustergültig vorleben, damit er funktioniert! Dies gilt es gerade trotz des allgegenwärtigen Drucks des Tagesgeschäfts zu beweisen [Kaplan and Mikes(06.2012), vgl. S.5]. Präventive Methoden sind meist schwer messbar, doch gerade sie sind es, die ein erfolgreiches Unternehmen ausmachen!

3.10 Information, Kommunikation und Berichterstattung im Risikomanagement

Zusammenfassung der Risikoberichterstattung und -kommunikation wie sie in dieser Arbeit verstanden wird:

$Das\ ist$ "Relevante Informationen werden ermittelt, erfasst und in einer solchen Form und einem solchen zeitlichen Rahmen kommuniziert, dass alle Beteiligten ihren Verantwortlichkeiten nachkommen können" [COSO(2006), vgl. S.75ff]. Die Risikoberichterstattung ist nicht Teil des Risikomanagementprozess Regelkreises, sondern ein unterstützender Prozess [Diederichs(2012), vgl. S. 163].

$Kriterium\ 1$ Die Kommunikation soll generell präzise und zielgerichtet im Unternehmen erfolgen, mit besonderem Augenmerk auf eine klare Sprache beim Risikomanagement. Allen Mitarbeitern wurde das Risikomanagement mitgeteilt und verständlich gemacht, z.B. mittels Handbuch siehe Abschnitt 4.1. Offene Kommunikationskanäle bestehen im Unternehmen. Die externe Kommunikation erfolgt vorschriftsgemäß [COSO(2006), vgl. S.71ff].

$Kriterium\ 2$ Aus externen und internen, aktuellen und vergangenen und Mikro-, und Makrorohdaten sollen sachdienliche Informationen werden. Dabei gilt, dass Informationen verlässlich und aktuell sein müssen [COSO(2006), vgl. S.67ff].

Abschnitt	Inhalt
Brief der Geschäftsführung	- Präsentation der Einstellung der Geschäftsführung zur Wichtigkeit von Integrität und Ethik im Unternehmen - Einführung in den Verhaltens- und Ethikkodex (Zweck und Anwendung)
Ziele und Philosophie	Darstellung der - Kultur, - Geschäftstätigkeit und Branche - Geographischen Standorte (national und international) - Bekenntnis zu ethischen Führungsverhalten
Interessenskonflikte	- Adressierung von Verhaltenskonflikten und Arten der Selbstkontrahierung - Adressierung von Mitarbeitern und im Auftrag des Unternehmens handelnden Personen sowie Aktivitäten, Investitionen oder Interessen, die Auswirkungen auf die Unternehmensintegrität oder Unternehmensreputation haben
Geschenke und Zuwendungen	- Adressierung der Vergabe von Geschenken und Zuwendungen unter Betonung der Unternehmensrichtlinie, die über die nationale Gesetzgebung hinausgeht - Etablierung von Standards und Anweisungen zum Umgang mit Geschenken und Bewirtung sowie deren angemessene Berichterstattung
Transparenz	Berücksichtigung von Regelungen zur Sicherstellung der Unternehmensverpflichtung für eine vollständige und verständliche soziale, ökologische und ökonomische Berichterstattung
Unternehmensressourcen	Berücksichtigung von Regelungen im Umgang mit Unternehmensressourcen, einschließlich geistigen Eigentums und geschützten Informationen - wem diese gehören und wie sie gesichert werden

Tabelle 3.8: Beispielhafter Verhaltens- und Ethikkodex nach [Bungartz(2012), Tab. 1]

$Kriterium\ 3$ Ein für das Unternehmen passendes Informationssystem wie in Kapitel 5 geschildert.

$Kriterium\ 4$ Die Berichterstattung handelt von Informationslogistik (siehe Abschnitt 5.4) und den 6 W-Fragen. Beim Risikoreport soll nach [Denk(2008), vgl. S.143 und 144] eine Darstellung der Gesamt-Risikoposition erfolgen, den Toprisiken und dem Maßnahmenplan.

$Ziel$ Sicherstellung, dass der Informationsfluss aller wesentlichen Risikoinformationen die richtigen Stellen erreicht [Denk(2008), vgl. S.134].

Bei COSO II ist dies in der Komponente Information und Kommunikation behandelt. Bei ISO 31000 ist die Risikoberichterstattung erneut jeweils im Risikomanagementprozess (Kp.5.2) und -rahmen (Kp. 4.3.6 und 4.3.7) beschrieben. Die Information und Kommunikation beschäftigt sich derzeit zu einem wesentlichen Teil mit dem **Aufbau eines Informationssystems** wie in Kapitel 5 und Kapitel 6 beschrieben. Da die Berichterstattung keinen spezifischen Risikomanagement Bezug hat, wird auf eine nähere Erläuterung verzichtet.

Sogenannte " **Risk Assessment Sheets**" nach [Denk(2008), vgl. S. 98-99] werden in der praktischen Berichterstattung und Kommunikation des Risikomanagementprozesses in Abschnitt 4.5 verwendet. Die einzelnen Kategorien müssen an das jeweilige Unternehmen, seine Datenbankstrukturen, Datenverfügbarkeit und Geschäftsprozesse angepasst werden. Vorlagen für die schnelle Umsetzung mittels Standardprozessen und -dokumenten sind bei Beratungsunternehmen oder Universitäten zu finden [17].

Eine detaillierte Arbeit über die Besonderheiten des angloamerikanischen risk-reporting findet man in [ICAEW(1997)].

3.11 Risikoüberwachung

Zusammenfassung der Überwachung wie sie in dieser Arbeit verstanden wird:

$Das\ ist$ Die Überwachung stellt sicher, dass das gesamte Risikomanagementsystem wirkungsvoll ist und überprüft somit als unabhängige 3. line-of-defense (LoD) die Arbeit des Risikomanagementsystems der 1. und 2. LoD. Berichtet wird mindestens den Aufsichtsgremien, meist werden Berichte über die normalen Geschäftstätigkeiten an die Vorgesetzten weitergegeben [COSO(2006), vgl. S.75ff]. Die Überwachung wird durch passende Richtlinien und systematische, regelmäßige und außernatürliche Kontrollaktivitäten umgesetzt. Es zielt auf eine effektive und effiziente operative Geschäftstätigkeit hin und sichert den Unternehmenswert [Bungartz(2012), vgl. S. 57].

$Kriterium\ 1$ Leistung des Risikomanagement anhand von Indikatoren laufend messen und den Fortschritt des Risikomanagement Entwicklungsplans überwachen [ISO(2009), vgl. S.21].

[17] http://www3.imperial.ac.uk/estatesprojects/projectprocedures/processes/pm/1.20(24.02.2014)

$Kriterium\ 2$ Überprüfung ob aufgrund der internen und externen Umwelt das Risikomanagement noch angemessen ist und einen Bericht über Schwachstellen verfassen. Die Informationsquellen im Unternehmen gilt es zu finden oder aufzubauen [COSO(2006), vgl. S.75ff].

$Kriterium\ 3$ Die Effektivitätsrisiken des Risikomanagementsystems verantwortet die Überwachung.

$Kriterium\ 4$ Gesonderte und außernatürliche Beurteilungen um die Effektivität und Glaubwürdigkeit des kompletten Risikomanagementsystems festzustellen, denn für die Effektivitätsrisiken ist die Überwachung zuständig [ISO(2009), vgl. S.21].

$Ziel\ ++$ Auffindung der Schwächen des Risikomanagementsystems im Unternehmen.

$Ziel\ +$ Schaffung weiterer unabhängiger Kontrollinstanzen im Unternehmen und Verantwortung für die Effizienzrisiken.

Da die Überwachung zwar einen spezifischen Risikomanagement Bezug hat, jedoch ein eigenes Themenfeld punkto Unternehmensaufsicht und Wirtschaftsprüfung darstellt, wird auf eine nähere Erläuterung verzichtet. Die Überwachung kann je nach Unternehmen etwa durch das interne Kontrollsystem, interne Revision oder einem Gremium im Aufsichtsrat erfolgen, siehe Kapitel Abschnitt 3.4.

Überprüfung der Compliance

Zumindest das Compliance und die interne Revision gehören in die Überwachung mit einbezogen oder mit dieser abgestimmt, siehe Abschnitt 3.4. Andere branchenspezifische Abteilungen sollten je nach Branche z.B. die Lebensmittelsicherheit und Arbeitssicherheit, beteiligt sein.

Für die Unternehmensführung sind die Zehn Fragen über die aktuelle Compliance Situation entscheidend [ERNST&YOUNGS(2012), vgl. S.9ff]:

1. Wird der richtige tone-at-the-top kommuniziert?
2. Werden Korruptionsrisiken effektiv ermittelt?
3. Gibt es effektive Richtlinien und Prozesse um die Risiken zu behandeln?
4. Werden die Manager passend informiert und geschult über Betrug, Korruption und Compliance?
5. Wird der Erfolg von Schulungen überprüft?
6. Welche Anreize gibt es für compliance gerechtes Verhalten und welche Strafen für nicht compliance gerechtes Verhalten?
7. Wie wird mangelnde Compliance überwacht und überprüft?

8. Hat die Unternehmensweite 3. LoD (line-of-defense) eine passende Schlagkraft, Ressourcen und Unabhängigkeit?
9. Wie wird die Effektivität der 3. LoD ermittelt?
10. Wenn Probleme gefunden werden, wie wird eine unabhängige und vollständige Untersuchung sichergestellt?

Nach einer Studie, die Compliance in 173 Unternehmen des Mittelstandes untersucht, sind folgende Hinweise lohnend:

- 80% der Unternehmen beschäftigen sich mit Compliance. Wobei ein Compliance Management nur in 48% der Unternehmen existiert und in weiteren 18% geplant ist [Reiß and Reker(2011), vgl. S.8]. 83% der Compliance Beauftragten führten dies in Personalunion mit einer anderen Funktion aus. 75% waren Geschäftsführer oder Vorstände, 17% Verwaltungs- oder Kaufmännische Leiter und 8% Leiter der Rechtsabteilung [vgl. S.19]deloitte2011.
- Der Nutzen der Compliance wird durch verbesserte Transparenz, Schadensvermeidung, Führungsverhalten und Mitarbeitervertrauen angegeben [Reiß and Reker(2011), vgl. S.12].
- Nur 65% der Compliance Abteilungen beschäftigen sich mit Prävention und 43% mit Korrekturmaßnahmen [Reiß and Reker(2011), vgl. S.13].
- 73% der Unternehmen ahnden Verstöße, 60% leiten an Strafverfolgungsbehörden weiter, 31% haben standardisierte Vorgehensweisen und 28% ein anonymes Hinweissystem als benutzte Sanktionierungsmechanismen [Reiß and Reker(2011), vgl. S.18].
- In Deutschland sind über 1.800 Gesetze mit 55.000 Einzelnormen in der Bundesrechtsdatenbank (Stand 24.09.2007) verzeichnet. Deswegen sind spezialisierte Bereiche im Unternehmen eine praktische Notwendigkeit [Reiß and Reker(2011), vgl. S.11].

KAPITEL 4

Praxisbericht eines unternehmensweiten Risikomanagementsystem

Das komplette Kapitel befasst sich mit der Anwendung der Risikomanagement Grundlagen aus Kapitel 3 in Form eines internen Handbuchs. Es spiegelt somit die für die Anwendung und Gesetzgeber notwendigen Schritte wieder.

Dieses Handbuch soll im Sinne der betroffenen Nutzer geschrieben werden und eine übersichtliche und gut lesbare Beschreibung des firmenweiten Risikomanagements bieten. Der tägliche Gebrauch des Handbuchs ist dafür ein wichtiges Qualitätsmerkmal.

Das folgende Kapitel kann bereits als Vorlage für ein mittelständisches Risikomanagementhandbuch dienen und soll schlussendlich alle unternehmensspezifischen Risikoprozesse und -vorgaben beinhalten.

4.1 Grundsätze des Risikomanagementhandbuchs

Das Risikomanagementhandbuch unterstützt die im Risikomanagement tätigen Personen (insbesondere Risikomanager und Risikoeigner) bei der Erfüllung ihrer Aufgaben. Es folgt den beiden gängigen Normenwerken COSO II Enterprise Risk Management Framework und ISO 31000.

Führungskräften und Mitarbeitern des Unternehmens dient es als Nachschlagewerk und stellt eine zusammenfassende Organisationsrichtlinie für das Risikomanagement dar. Das vorliegende Handbuch regelt die wichtigsten Elemente des Risikomanagementsystems, insbesondere:

- Definiert Kapitel 0 die verwendeten Begriffe.

- Erläutert Kapitel 1 die Grundsätze des Risikomanagements und deren strategische Vorgaben in Form der Risikomanagement-Politik.
- Kapitel 2 dient zu Regelungen der Aufbau- und Ablauforganisation, Kompetenzordnung und der Verantwortlichkeiten. Schnittstellen zwischen dem Risikomanagement und anderen Abteilungen werden erläutert.
- Kapitel 3 beschreibt das Konzept zur Risikosteuerung im Unternehmen, hinsichtlich der
  - Erklärung der verwendeten Methoden
  - Einteilung der Risiken in Kategorien
  - Ausgestaltung von Prozessen für die Risikobewertung und -steuerung,
  - Risikoberichterstattung und Kommunikation innerhalb des Risikomanagements
  - Abgrenzung zwischen internen Kontrollsystemen, Compliance und interner Revision
- Kapitel 4 zeigt die Umsetzung des Risikomanagementsystem mittels Software.
- Schließlich legt es die Geltungsbereiche, Inkraftsetzung, gesetzliche Regelungen und Versionierung fest (vgl. Kapitel 5).

Die Vorgaben sind notwendig, um eine einheitliche Umsetzung des Risikomanagements und eine konsolidierte Berichterstattung konzernweit zu ermöglichen. Das Handbuch wird aufgrund aktueller Bedürfnisse periodisch angepasst und weiterentwickelt.

Das Risikomanagement besteht aus zwei Kreisläufen. Dem Risikoprozess nach Kapitel 3 als Innenansicht, in dem Risiken von Identifikation über Bewertung bis hin zur Kontrolle zyklisch bearbeitet werden. Zweiter Kreislauf ist der Risikorahmen nach Kapitel 1 als Außenansicht, der das Umfeld, Kultur, Leitbild, Ziele und Strategie des Unternehmens beschreibt.

4.2 Kapitel 0 - Begriffsdokumentation

Grundlage eines proaktiven (ex post) und effizienten Risikomanagementsystems ist eine transparente und verständliche Kommunikation. Die gemeinsame Risikosprache ist dabei genauso wichtig, wie eine gemeinsame Kommunikationsebene im Unternehmen, z.B. ein Newsletter oder regelmäßige Besprechungen. In diesem Abschnitt werden die im Unternehmen verwendeten Begriffe klar definiert und abgegrenzt.

Für die Begriffsdefinition sind hier folgende Beispiele in alphabetischer Reihenfolge aufgelistet:

Begriff	**Beschreibung**

Angemessenheit	Es wird darunter die Verhältnismäßigkeit zwischen dem Aufwand und dem Ergebnis verstanden. Z.B. werden Risiken unterhalb von 5 TEUR pro Jahr nicht betrachtet oder aufwändige Analysen nur bei Toprisiken erstellt.
Ausprägung	Im Konzern sind die von den MitarbeiterInnen im Workshop oder Umfragen getätigten Aussagen über ein Risiko, die Ausprägungen. Sie beschreiben noch detaillierter wie Ereignisse in der jeweiligen Praxis vorkommen. Die Ausprägung ist ein Beispiel des individuellen Ereignisses. Sie spiegeln bildhaft die jeweils reale Situation und Sprache vor Ort wieder. Im Konzern tragen viele Bereiche das Risiko der Arbeitssicherheit, doch die konkreten Situationen werden unterschiedlich sein und sind somit Ausprägungen. Für eine konzernweite Verwendung wird jede Ausprägung einem passendem Ereignis in der Risikokategorie zugeordnet, so wird z.B. die Ausprägung Staplerkörbepflicht, dem Ereignis Arbeitssicherheit zugeteilt.
Bedeutung	Umfang eines Ereignisses oder einer Entwicklung, die zu einer Beeinträchtigung der Ziele oder der Aufgabenerfüllung führt.
Bestands-gefährdung	Sollten Ereignisse eine Bestandsgefährdung aufweisen, sind sie als Toprisiken zu markieren.
Chance	Eine Chance ist die Prognose einer positiven Abweichung von einem vorab definierten und erwarteten Zielwert und somit die Möglichkeit eines unerwarteten Nutzens bzw. Gewinnes. Im Risikomanagement werden diese separat betrachtet und idealerweise mit konkreten Maßnahmen vorschlagen.
Compliance	Ist die Abteilung die für die Einhaltung von Gesetzen und Richtlinien, aber auch von freiwilligen Kodizes, in Unternehmen zuständig ist. Siehe Seite Abschnitt 3.4 usw.
Ereignis	Da das Risiko auch Chancen beinhaltet, werden beide Begriffe allgemein Ereignis genannt. Eintritt oder Veränderung einer bestimmten Kombination von Umständen. Unser Unternehmen versteht darunter den wesentlichen Überbegriff einer Kategorie von Vorkommnissen. Z.B. Arbeitssicherheit in der operativen-, Marktanteil in der strategischen- oder Einkaufpreis in der wirtschaftlichen- Kategorie. Somit sind Ereignisse Sammelbecken für mehrere Ausprägungen, die für eine oder mehrere Abteilungen zutreffen. Im Risikomanagementsystem werden Ereignisse von Risikoexperten und Risikomanagern gepflegt.

Häufigkeit	Häufigkeit des Eintritts zukünftiger Ereignisse oder Entwicklungen (objektive Definition). Unsicherheit von Aussagen bzw. Grad der persönlichen Überzeugung, betreffend dem Eintritt eines Ereignisses oder einer Entwicklung (subjektives Verständnis). Die Wahrscheinlichkeit eines Risikos kann sich auf eine Periode (z. B. Jahreswahrscheinlichkeit) oder auf eine Anzahl von Fällen (Fallwahrscheinlichkeit) beziehen.
Individuelles Ereignis	Man versteht darunter ein Ereignis, das genau für eine Abteilung angewendet und bewertet wurde. Ein Beispiel wäre das Kreditausfallrisiko in der Tochter A mit ausschließlich Kleinkunden, welches nicht vergleichbar ist gegenüber dem Kreditausfallrisiko der Tochter B mit Großkunden Inland und auch nicht mit jenem der Tochter C Großkunden Ausland. Dies wird in Abbildung Abbildung 4.14 gezeigt, es ist nicht sinnvoll für alle drei Tochterfirmen eigene Risiken getrennt voneinander anzulegen. Denn sie weisen Ähnlichkeiten in Modell, Experten, Maßnahmen, Quellen oder Verantwortungsbereich auf und sind somit sinnvollerweise von Anfang an in enger Abstimmung zu behandeln. Im Risikomanagementsystem spiegelt das individuelle Ereignis die Grundeinheit (kleinste Einheit) im Risikomodell wider und ist somit auch im Datenmodell der zentrale Verknüpfungspunkt vieler anderer relevanter Prozesse, Daten und Modelle. Gedanklich kann jedes individuelle Ereignis als einzelnes Risikostammblatt gesehen werden. Die genaue Einteilung der Risiken ist für die Weiterarbeit mit Risikomodellen, Berichterstattung und Folgewirkungen wichtig. Im Risikomanagementsystem werden individuelle Ereignisse von den Risikoeignern gepflegt, unter Anwendung der Vorgaben.
Internes Kontrollsystem	Das IKS überwacht alle organisatorischen und technischen Maßnahmen die in der Organisation eingeführt wurden. Das IKS bei uns konzentriert sich insbesondere auf die operativen Geschäftsprozesse, siehe Kapitel 2.
Maßnahme	Verfahren zur Veränderung und Bewältigung von Risiken. Maßnahmen lassen sich grob unterteilen: Eingehen oder Steigerung des Risikos zur Nutzung einer Chance; Beseitigung der Risikoquelle; Veränderung der Wahrscheinlichkeit oder Auswirkungen; Teilung des Risikos durch Verträge oder Vermeidung von Risiken oder sogar als jene Maßnahmen indenen die Aktivität komplett eingestellt wird.
Risiko	Risiko ist die Prognose einer möglichen negativen Abweichung von einem vorab definierten und erwarteten Zielwert, es besteht die Gefahr eines Schadens bzw. Verlustes. Ein Risiko berechnet sich in der simpelsten Form aus der Eintrittswahrscheinlichkeit multipliziert mit dem zu erwarteten (finanziellen) Ausmaß.

Reines Risiko	Reine Risiken haben ausschließlich einen negativen Ausgang, z.B. Erdbeben. Sie können nur versichert oder mit Katastrophenplänen vorbereitet werden, enthalten aber kein Chancenpotential.
Restrisiko	Bestehende Risiken einer Organisation, die nach der Identifikation und Zuteilung einer Maßnahme im Unternehmen verbleiben.
Risikokategorie	Unterteilung von Ereignissen nach unterschiedlichen Kriterien. Bei uns sind diese in 5 Kategorien unterteilt: Operative, Strategische, Wirtschaftliche, Reporting und Compliance.
Risikokomitee	Ist eine Gruppe von Risikoexperten, die bei Aufgaben und Entscheidungen den Risikomanager unterstützt . Regelmäßige Treffen dieser Gruppe, bei der die Toprisiken besprochen, Risikoreports freigegeben und Entscheidungen bezüglich des Risikomanagementsystems getroffen werden. Das Komitee setzt sich aus Entscheidungsträger (ein Vorstand) und den zuständigen Stabsstellen (Risikomanagement, Compliance, IKS, Controlling) zusammen.
Risikostammblatt	Für jedes individuelle Ereignis einer eigenständigen Abteilung wird ein Stammblatt ausgefüllt. Dies beinhaltet die persönliche Einschätzung und Situation des Risikoeigners. Im Risikomanagementsystem sind Stammblätter Formulare mit auswählbaren Datenbankeintragungen im Hintergrund, somit ist der Schreibaufwand minimal.
Risikoeigner	Sind die in den Abteilungen zuständigen Führungspersonen, die Verantwortung verbleibt bei ihnen, selbst wenn ein lokaler Risikoverantwortlicher bestimmt worden ist.
Risikoexperte	Jedes Ereignis sollte einen zugewiesenen Experten haben, der die fachliche Bewertungsmethode vorgibt, die neuen individuellen Ereignisse oder Ausprägungen freigibt oder deren Ergebnisse auf Sinnhaftigkeit überprüft. Weiters ist er die Ansprechperson des Risikomanagers.
Risikomanager (Zentraler)	Sind Mitarbeiter der Stabsstelle Risikomanagement (RM) in unserem Unternehmen, siehe Kapitel 2.
Risikoaggregation	Das Verfahren, das mehrere Risiken auf übergeordneter Ebene zusammenfasst. Die Berichterstattung und zum Teil die Steuerung des aggregierten Risikos, erfolgen dann auf dieser übergeordneten Ebene.
Risikolandkarte bzw. -matrix	Darstellung, in der Risiken entsprechend ihrer Bedeutung und der Eintrittshäufigkeit graphisch in einen 4x4 Raster eingeordnet werden.

Toprisiko	Nach der Identifikation und Bewertung der vielen, teils unbedeutenden, Risiken, werden die wenigen, für die Konzernleitung wesentlichen Risiken, separat markiert. Dies sind z.B. die größten Risiken je Abteilung oder alle Risiken, die eine definierte Risikohöhe überschreiten. Für Toprisiken werden schrittweise Detailanalysen erfolgen und jeweils ein passendes Risikomodell erstellt werden, welches zuverlässigere Vorhersagen, Simulationen und bestenfalls quantitative Euro-Werte liefert.
Verbesserungspotential	Verbesserungsvorschläge die während des Risikoprozesses entstehen. Diese werden als Teil einer kontinuierlichen Verbesserung im System geführt und sind somit am Stammblatt sichtbar. Sie sind jedoch für das Risikomanagement nicht relevant.
Wesentlichkeit	Die Wesentlichkeit eines Risikos wird plakativ mit der Frage beschrieben: Hätte jemand wirtschaftliche Entscheidungen anders getroffen, hätte er das Risiko gekannt? Wenn diese Frage mit einem Ja zu beantworten ist, dann liegt ein wesentliches Risiko vor.

Tabelle 4.1: Beispielhafte Übersicht der spezifisch im Unternehmen verwendeten Risikobegriffe

4.3 Kapitel 1 - Übersicht des unternehmenseigenen Risikomanagementrahmen

Dem hier aufgeschlüsselten Kapitel liegen Theorien nach Abschnitt 3.3 zu Grunde.

Beispielhafte Risikopolitische Grundsätze für Industrieunternehmen

Die folgenden Definitionen sind die praktische Umsetzung des Abschnitt 3.3 für einen Industriebetrieb.

- **Risikobewusstsein und Bekenntnis zur aktiven Teilnahme** - In allen Unternehmensbereichen muss sich der Mitarbeiter bewusst sein, dass das Risikoumfeld seines Verantwortungsbereiches durch seine Handlungen beeinflusst und mitgestaltet wird. Es besteht daher ein ausdrückliches Bekenntnis zur aktiven Teilnahme am Risikomanagement. Unser Geschäft ist untrennbar mit dem Eingehen und dem Abwägen von Chancen und Risiken verbunden. Kenntnis dieser Risiken und die Steuerung ihrer Auswirkungen auf unsere Kunden und unsere Gesellschaft ist entscheidend.

- **Maßgeblichkeitsprinzip** - Aktivitäten des Risikomanagement folgen dem Maßgeblichkeitsprinzip im Sinne einer Relevanzeinschätzung potentieller Ereignisse hinsichtlich Eintrittswahrscheinlichkeit und Auswirkungen. Um eine Überbürokratisierung zu vermeiden wird eine Mindesthöhe vorgeschrieben, die ein Risiko erreichen muss.

- **Subsidiaritätsprinzip** - Das zentrale Risikomanagement zeichnet sich zuständig für Prinzipien, Methoden, Verfahren, Limite und Anweisungen. Die leitenden Mitarbeiter und Geschäftsführer sind als Risikoeigner verantwortlich für die ordentliche Behandlung der in ihren Bereich auftretenden Risiken und Chancen. Diese operativen Aufgaben der Risikoidentifikation und Risikosteuerung werden somit grundsätzlich dezentral durchgeführt, im Sinne einer hohen Reaktionsgeschwindigkeit und der Nutzung von lokal verfügbaren Expertenwissen. Findet eine Aufgabenstellung keine Deckung im vorgegebenen Ziel-, Kompetenz- und Limitsystem, so hat der konzernweite Risikomanager umgehend eine entscheidungsbefähigte Stelle einzurichten. Das bedeutet, man sollte fragen wenn man sich nicht auskennt!

- **Objektivierung** - Wir streben ein größtmögliches Maß an Objektivität, Transparenz und Nachvollziehbarkeit in der Messung, Steuerung und Limitierung von Risiken an.

- **Sanktion** - Es erfolgt beim Risikoverantwortlichen keine Sanktion von Schadensereignissen, sondern lediglich von Unterlassung und Verstößen gegen die Prinzipien des Risikomanagement. Das bedeutet unabhängig von einem Schadenseintritt wird beurteilt ob das Verhalten und die Einschätzung korrekt waren oder ob sie z.B. beschönigt oder ignoriert wurden.

- **Klarheit der Organisation** - In unserer Auf- und Ablauforganisation ist klar und eindeutig geregelt, wer was, wann und nach welchen Prinzipien zu tun hat.

- **Normgerechte Gestaltung des Risikomanagements** - Die Ausgestaltung des unternehmensweiten Risikomanagementsystems folgte durch die den Empfehlungen des COSO II Framework und der ISO 31000.

Beispielhafte Visionen und Ziele des Risikomanagements für Industrieunternehmen

Dieses Kapitel ist die praktische Umsetzung der Theorien aus Abschnitt 3.3.

Unternehmerisches Handeln ist in der heutigen Zeit, ohne das Eingehen von Risiken nicht denkbar. Primäres Ziel ist es nicht, anfallende Risiken zur Gänze auszuschalten oder zu eliminieren, da dabei mögliche Chancenpotentiale ungenutzt bleiben könnten. Vielmehr sollte das Erreichen und Sicherung einer risikooptimalen Unternehmensposition angestrebt werden.

Statt der Minimierung von Risiken liegt die Aufgabe eines erfolgreichen Risiko- und Chancenmanagements vor allem im Schaffen von Transparenz über die Risikosituation im Unternehmen und dem optimalen Umgang mit den identifizierten Risiken und Chancen.

Im Kontext des Risiko- und Chancenmanagements ist somit das spekulative Risiko von großer Bedeutung und insbesondere folgende Fragen ausschlaggebend:

- Welche Faktoren bedrohen Erfolg und Erfolgspotenziale? Erfolgspotenziale, wie Kernkompetenzen, interne Stärken und Wettbewerbsvorteile, sind Voraussetzungen für zukünftige Gewinne bzw. cashflows.

- Welche Kernrisiken soll das Unternehmen selbst tragen? Als Kernrisiken werden jene Risiken bezeichnet, die im unmittelbaren Zusammenhang mit dem Aufbau bzw. der Nutzung von Erfolgspotenzialen stehen und nicht auf andere übertragen werden können.

Weitere Ziele des Risikomanagementsystems:

- Sicherung der Existenz und künftiger Erfolg des Unternehmens
- Optimierung der Risikokosten, insbesondere der mittel-, und langfristigen Risikokosten.
- Relevante gesetzliche und regulatorische Anforderungen, sowie internationale Normen einzuhalten
- Die relevanten Risiken zu kennen und zu bewerten
- Einflussfaktoren (Risikotreiber) und Wirkmechanismen transparent zu machen
- Verfügbarkeit und Einsatz adäquater Mechanismen zur Risikobewältigung

Visionen des Risikomanagements:

- Schrittweise und kontinuierliche Verbesserung des konzerneigenen Risikomanagementsystems hin zu einem hohen Reifegrad und quantifizierten Risikomaß
- Verankerung eines Risikobewusstseins bei allen Beteiligten und Prozessen
- Gelebte Früherkennung von drohenden Gefahren für deren rechtzeitige Abwendung (siehe Abschnitt 3.8)
- In einem hochentwickelten Risikomanagement wird künftig ein Performancemaß als Basis für eine risikoorientierte Unternehmenssteuerung nötig werden. Diese würde eine Abwägung zwischen Ertrag und Risiko ermöglichen.

Beispielhafte gesetzliche Regelungen für Industrieunternehmen

Dieses Kapitel ist die praktische Umsetzung der Theorien aus Abschnitt 2.2.

Gesetzliche Bestimmungen die spezialisierte Themen beinhalten, so z.B. Compliance, Datenschutz oder Lebensmittelsicherheit, werden im Konzern gesondert von eigenen Verantwortlichen abgehandelt. Folgende österreichische Gesetzte erfordern ein adäquates Risikomanagementsystem im Unternehmen, siehe Tabelle 2.1.

Grundlegende Methoden des unternehmensweiten Risikomanagementsystems für Industrieunternehmen

Die Grundgestaltung des konzernweiten Risikomanagementsystems ist an ISO 31000 und COSO ERM II angelegt. Die ISO 31000 Norm geht weitestgehend mit jenen der österreichischen Umsetzung ONR 49000 bis 49003 einher und ist ebenfalls im Aufbau nahezu ident mit dem COSO Framework. Eine genauere Beschreibung wird im Abschnitt 2.2 und Abschnitt 3.3 gegeben.

Beim Risikomanagement nach ISO 31000 und COSO II legt die Geschäftsführung anhand des Risikomanagementrahmens die Ziele fest. Dezentral werden im Zuge des Risikomanagementprozesses Ereignisse als Risiken oder Chancen identifiziert, bewertet und bewältigt. Parallel findet eine Überwachung seitens des zentralen Risikomanagers statt, der auch Methoden vorgibt und Reports für den Vorstand erstellt. Die Abbildung beider Modelle findet man in Abbildung 2.2 und Abbildung 2.3.

Gutes Risikomanagement zielt nicht darauf ab Risiken um aller Kosten willen zu vermeiden, sondern soll in Anbetracht der Unternehmensziele informierte Entscheidungen über chancenreiche und ungewollte Risiken ermöglichen, [ERNST&YOUNGS(2010), S.1]!

Es gibt eine Vielzahl an speziellen Methoden, wie in Abschnitt 4.5 gezeigt. Grundlegende Methoden sind ein Bekenntnis zur kontinuierlichen Verbesserung des Risikomanagements und eine Organisationsstruktur die dem 3-lines-of-defence Modell mit einem Zusammenspiel von Risikoeigner, Compliance, Risikomanagement, internen Kontrollsystem und interner Revision folgt, siehe Abschnitt 4.4 . Spezialisierte Themen wie z.B. die Abdeckung der diversen öffentlichen Gesetze bzw. deren Bescheid-Verwaltung (legal-care) oder die Lebensmittelsicherheit (HAACP), werden gesondert von eigenen Verantwortlichen abgehandelt.

4.4 Kapitel 2 - Aufbau und Organisation

Dem hier aufgeschlüsselten Kapitel liegen Theorien nach Abschnitt 3.4 zu Grunde.

Aufbauorganisation

Die Aufgaben im Risikomanagement werden im Konzern zentral organisiert und dezentral umgesetzt. Die gemeinsame Stabstelle für Risikomanagement und Compliance ist für die Koordination, unternehmensweites Konzept und Methoden zuständig. Weiters folgt das Risikomanagement prinzipiell dem in Abschnitt 4.3 beschriebenen Subsidiaritätsprinzip. Die direkt im Prozess Verantwortlichen sind für dessen Risiken und Umsetzung der Maßnahmen selbst zuständig. Mehrere Stellen im Unternehmen tragen für spezielle Teilbereiche die alleinige Verantwortung, siehe Verantwortlichkeiten im Abschnitt 4.4. In diesem Kapitel werden die beteiligten Stellen, deren Position im Unternehmen und Berichtswege aufgelistet.

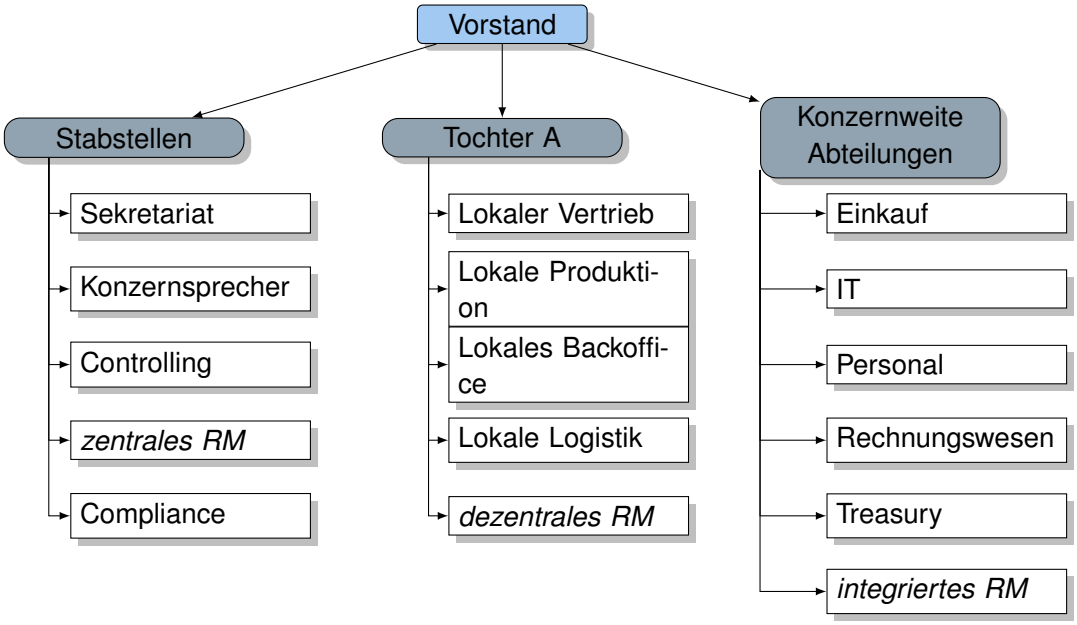


Abbildung 4.1: Beispielhaftes Organigramm eines Industrieunternehmens

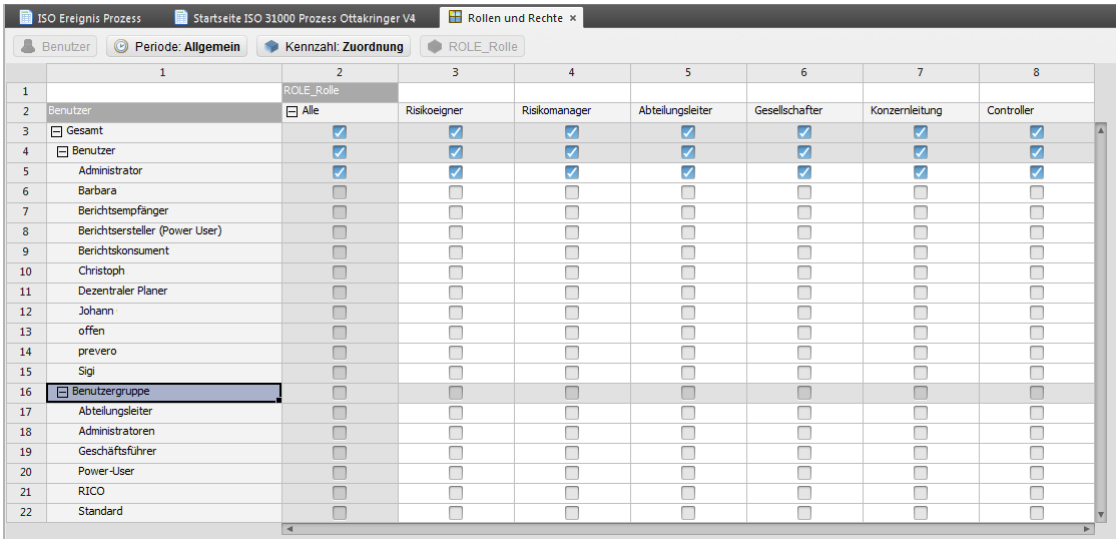
Es wird empfohlen ein Organigramm des Unternehmens vergleichbar mit Abbildung 4.1 und Abbildung 4.3 anzufügen, um übersichtlich das Risikomanagement von allen angrenzenden Einheiten wie dem interne Kontrollsystem und interne Revision abzugrenzen.

Einbettung des Risikomanagements in die Geschäftsprozesse

Das Risikomanagement wird als wichtiges Führungsinstrument im Konzern gesehen und ist ein fester Bestandteil der Geschäftsprozesse und Zielvorgaben. Nach aktueller gesetzlicher Regelung gehört es zu den Sorgfaltspflichten einer ordentlichen Geschäftsführung. Insbesondere ist es auf allen Stufen des Unternehmens einzubeziehen.

- Strategie- und Planungsprozesse - Mit den jährlich festgelegten Zielen der Geschäftsführung soll rechtzeitig auf Veränderungen des Umfelds reagiert werden. Das Risikomanagement unterstützt die Geschäftsführung mit regelmäßigen Risikoanalysen und kontinuierlichen Verbesserungsmaßnahmen.

- In einzelnen Abteilungen oder Unternehmen sind spezielle Prozesse nötig, wie das IKS, Qualitätsmanagement, Umweltmanagement, Arbeitssicherheitsmanagement, Lebensmittelsicherheit oder der IT-Security. Synergien zwischen diesen Prozessen und Risikomanagement müssen gefunden und genutzt werden. Zumindest ist ein Informationsaustausch sicherzustellen.



	1	2	3	4	5	6	7	8
1		ROLE_Rolle						
2	Benutzer	Alle	Risikoeigner	Risikomanager	Abteilungsleiter	Gesellschafter	Konzernleitung	Controller
3	Gesamt	☑	☑	☑	☑	☑	☑	☑
4	Benutzer	☑	☑	☑	☑	☑	☑	☑
5	Administrator	☑	☑	☑	☑	☑	☑	☑
6	Barbara	☐	☐	☐	☐	☐	☐	☐
7	Berichtsempfänger	☐	☐	☐	☐	☐	☐	☐
8	Berichtsersteller (Power User)	☐	☐	☐	☐	☐	☐	☐
9	Berichtskonsument	☐	☐	☐	☐	☐	☐	☐
10	Christoph	☐	☐	☐	☐	☐	☐	☐
11	Dezentraler Planer	☐	☐	☐	☐	☐	☐	☐
12	Johann	☐	☐	☐	☐	☐	☐	☐
13	offen	☐	☐	☐	☐	☐	☐	☐
14	prevero	☐	☐	☐	☐	☐	☐	☐
15	Sigi	☐	☐	☐	☐	☐	☐	☐
16	Benutzergruppe	☐	☐	☐	☐	☐	☐	☐
17	Abteilungsleiter	☐	☐	☐	☐	☐	☐	☐
18	Administratoren	☐	☐	☐	☐	☐	☐	☐
19	Geschäftsführer	☐	☐	☐	☐	☐	☐	☐
20	Power-User	☐	☐	☐	☐	☐	☐	☐
21	RICO	☐	☐	☐	☐	☐	☐	☐
22	Standard	☐	☐	☐	☐	☐	☐	☐

Abbildung 4.2: Beispielhafte Verteilung der Verantwortung und Zugriffsrechte in einem Informationssystem durch einen Administrator

Verantwortlichkeiten, Rollenbilder und Tätigkeiten im Konzern

Die Zuteilung der Verantwortung und Zugriffsrechte im Konzern wird im Informationssystem durch den Administrator vergeben, wie beispielhaft in Abbildung 4.2 gezeigt.

Zusammenspiel Compliance, Risikomanagement und internes Kontrollsystem im 3-lines-of-defence Modell

Die Abbildung 4.3 ist die Umsetzung des theoretisch in Abschnitt 3.4 beschriebenen Modells. [1] Die Abkürzung GRC (engl. für governance-risk and compliance-system) dient meist als Überbegriff für IT-unterstützte Risikomanagement Plattformen.

Die Rollenverteilung im Bezug auf Risikomanagement und Kontrolltätigkeiten wird zunehmend auf mehrere Bereiche im Unternehmen verteilt. Unternehmen stehen demzufolge vor der Herausforderung, diese Aufgaben sorgfältig und klar zu koordinieren, um sicherzustellen, dass Risiko- und Kontrollprozesse angemessen funktionieren und keine Kontrolllücken oder Doppelarbeiten entstehen. Das in Abbildung 3.4 dargestellte three-lines-of-defense Modell bietet eine einfache und kompakte Darstellung der Rollenverteilung der einzelnen Risikomanagementfunktionen im Unternehmen.

1. Line-of-defense (LoD) bildet das operative Management bzw. der Risikoeigner. Dieser ist für den Risikoprozess der Identifizierung, Beurteilung und Kontrolle der Risiken

[1] Dabei dient das vorzügliche Risikomanagement der Österreichischen Post AG in Abbildung 4.3 als Beispiel, siehe `http://www.controller-forum.org/data/_uploaded/file/pdf/Vorträge%202014/01-Vortrag%202_Peter%20Umundum-Österreichische%20Post%20AG.pdf` (19.03.2014).

Rolle	Aufgabenbeschreibung
Aufsichtsrat	• Muss in der Lage sein, unabhängig zu sein und die Aktivitäten des Managements zu hinterfragen. • Beaufsichtigt das Risikomanagement und ist sich der Risikoappetite des Unternehmens bewusst und stimmt diesen zu. • Überprüft das Risikoportfolio und wiegt es gegen den Risikoappetit ab. • Kennt die Toprisiken und weiß ob das Management geeignete Maßnahmen ergriffen hat.
Geschäfts-führung	• Die Einrichtung und Sicherstellung eines funktionierenden Risikomanagementsystems gehört zur Haupt- und Letztverantwortung der Gesamtkonzern-Geschäftsführung. • Schafft durch den Risikomanagementrahmen ein positives internes Umfeld dem Risikomanagement gegenüber, der sogenannte tone-from-the-top.
Risikomanager in der Stabstelle Risikomanagement und Compliance	1. **Strategisches Risikomanagement** Unterstützung der Geschäftsführung bei strategischen Risiken Entwicklung des Risikomanagementprozesses Proportionalität und Konzernsicht Bewertungsmodelle Klassifizierungen 2. **Administration** Unterstützung der Risikoeigner Technischer Support Software Berechtigungen Schulungen Risikomanagementhandbuch 3. **Überwachung** Kontrolle der Maßnahmen Jahresgespräche mit Risikoeignern Einforderung der Umsetzung Früherkennung 4. **Reporting** Auswertungen, Analysen Aggregation der Ereignisse Proportionalität und Konzernsicht Kommunikation mit Geschäftsleitung Dokumentation der Historie
Risikoexperte	• Für einzelne Risikokategorien kann es sinnvoll sein, dass der Risikomanager einen Experten für die unternehmensweite Koordination dieser Risikokategorie definiert. Darunter fällt auch die Erarbeitung der Bewertung und Überprüfung der Bewältigung.
Risikoeigner	• Die für die einzelnen Abteilungen zuständigen Leiter sind verantwortlich für den Umgang mit Risiken, die mit Zielen ihres Unternehmensbereiches zusammenhängen. • Leiten Risikobewältigungsmaßnahmen ein
MitarbeiterInnen	• Von jedem Mitarbeiter wird ein entsprechendes Risikobewusstsein erwartet. Insbesondere müssen Gefahren dem Vorgesetzten gemeldet und Maßnahmen aktiv eingebracht werden. • Die Verantwortung des Mitarbeiters ist eine aktive Teilnahme am Risikomanagement, das ist direkt oder indirekt Teil jeder Stellenbeschreibung.

Tabelle 4.2: Verantwortlichkeiten und Rollenbilder im konzernweiten Risikomanagement

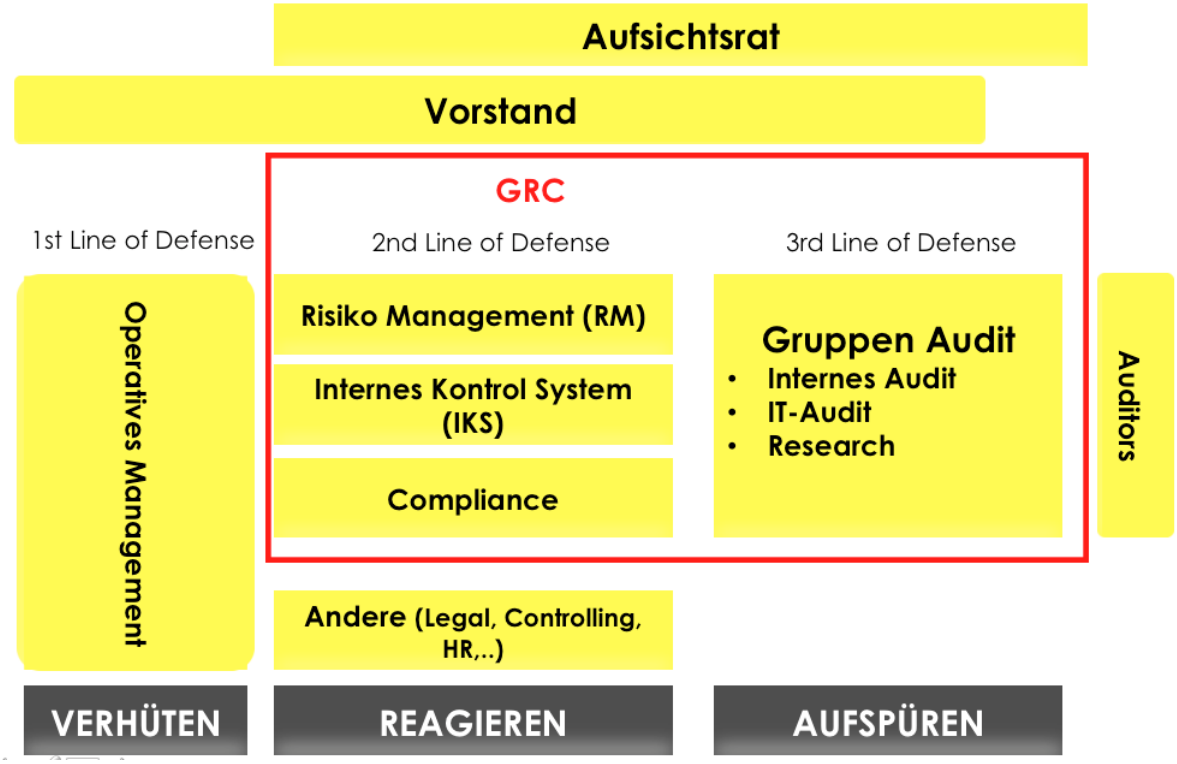


Abbildung 4.3: Beispielhafte Verankerung des three-lines-of-defense Modells im Unternehmen anhand der Österreichischen Post AG

während des Tagesgeschäfts verantwortlich.

2. LoD verantwortet den Überwachungsprozess mit kritischer Hinterfragung der Ergebnisse und ermöglicht wirksame Risikomanagementmethoden und -Werkzeuge. Es unterstützt die Risikoeigner bei offenen Fragen und in einigen Unternehmen wird für die Überwachung von Spezialrisiken zusätzlich auch eine separate Verantwortung geschaffen.

3. LoD ist als interne Revision die objektive und unabhängige Prüfungsinstanz, sie informiert und unterstützt die Unternehmensführung und Überwachungsgremien. Das Effektivitätsrisiko des unternehmenseigenen Risikomanagement wird verantwortet, ebenso wie Sicherheit, Angemessenheit und Wirksamkeit aller Überwachungs- und Kontrollstrukturen. Der Einsatz von “Executive Risk Committees” oder Risikoexpertengruppen zählt nach [Stegemann(Februar 2014), Exhibit 7] zur 3. LoD.

In Abbildung 3.4 wird aufgezeigt, wie im Unternehmen ein Qualitätsmanagement, IKS oder Prozessmanagement die Risikomanagementaufgaben in der Praxis übernehmen können aber auch, wie diese Abteilungen voneinander abzugrenzen sind und welche Synergien

sie aufweisen. Dabei wird speziell auf deren Ziele eingegangen, um die daraus resultierenden Risiken voneinander abgrenzen zu können. Somit ist es nicht wichtig, mit welcher Risikomanagementfunktion den einzelnen Risiken begegnet wird, sondern dass ein Unternehmen ihnen begegnet.

Existierender und angestrebter Reifegrad im Risikomanagementsystem

Die Grundlagen für Reifegrad-Modelle sind im Abschnitt 3.3 erklärt. Die in Tabelle 4.3 beurteilten Reifegrade verwenden die selben Gruppen wie in Abbildung 3.1, von Risikomanagement Politik, -Kultur, -Erfahrung, -Organisation, -Abteilungen bis -Prozess.

Das Risikomanagement (RM) kann mit verschiedenen Umfang und Reifegrad im Unternehmen eingesetzt werden. Die rechtliche Situation lässt für die konkrete Umsetzung genügend Spielräume, die Entscheidung über den künftig angestrebten Reifegrad obliegt somit der Geschäftsführung.

Die in der anschließenden Tabelle aufgelisteten Einstufungen geben typische Beispiele von Risikomanagementstufen in den verschiedensten Unternehmensfeldern. Zusammenfassend lassen sich die Stufen folgenderweise charakterisieren:

- Die Stufe 1 weist eine nicht mehr zu akzeptierende, natürliche Herangehensweise ans RM auf.

- Die Stufe 2 zeugt von einer strukturierten Herangehensweise, sowohl in der Beurteilung als auch Bewältigung und spiegelt einen gesetzlichen Mindeststandard wider, welcher fehlende Synergien aus dem RM vermuten lässt.

- Die Stufe 3 setzt quantitative, vollständige und normgerechte Umsetzung voraus. Das RM wird auf allen Unternehmensebenen gelebt und verfügt über notwendige Prozesse, technische Methoden und IT-unterstützte Werkzeuge.

- Die letzte Stufe 4 bedeutet, dass das RM den aktuellen technischen Entwicklungsstand genügt und einem integrierten Ansatz verfolgt. Dies spiegelt zwar den Stand der Forschung wider, erscheint für Industrieunternehmen jedoch übertrieben.

Für das rechtlich geforderte Risikomanagementsystem als Minimalumsetzung kann der Reifengrad in der zweiten Stufe herangezogen werden, dies listet den aus österreichischen Gesetzen ableitbaren Mindeststandard eines RM-Systems auf. Die Stufen 3 und 4 lassen sich als Empfehlungen zum Stand der Technik interpretieren, und spiegeln somit Schritte für eine weiterführende Umsetzung wider. Diesbezüglich sei erwähnt, dass das Risikomanagement entsprechend der spezifischen Organisationsformen, Unternehmenskultur und -zielen im Unternehmen aufgebaut werden muss. Es ist ausdrücklich darauf hinzuweisen, dass diese Strukturen einem mittelständischen Industrieunternehmen gleichen müssen und somit nicht mit Finanzunternehmen oder internationalen Konzernen vergleichbar sind. Gerade beim Risikomanagement ist eine schrittweise Umsetzung in mehreren Jahren empfohlen und nötig.

Die wesentlichen Tochterunternehmen und eventuelle Holdings sollten separat beurteilt werden. Um den derzeitigen Reifegrad in den einzelnen Schritten übersichtlich zu zeigen, können diese mit einem roten Kästchen in der folgenden Tabelle markiert werden.

4.5 Kapitel 3 - Ausgestaltung des Risikomanagementprozesses

Beim Risikomanagementprozess sind folgende typische Problemfelder nach [Gleissner and Mott(2008), vgl. S.63] und [pwc(2008), vgl. S.15ff] zu beachten. Die hier angeführten Methoden sollen dem Konzern helfen aussagekräftige und nützliche Resultate zu erhalten, bei einer minimalen Bürde innerhalb der Organisation:

1. Der interne Zusammenhang:
    - Der Risikomanagementrahmen und -Kultur muss etabliert sein, um den Risikomanagementprozess sinnvoll ausführen zu können [pwc(2008), S. 15].
    - Risikobeurteilung beginnt und endet mit der Betrachtung der spezifischen Ziele des Unternehmens [pwc(2008), S.15].
2. Risikoidentifikation:
    - Festsetzung und Beibehaltung einer fokussierten Systematik zur Risikoidentifikation (z.B. bottom-up oder top-down).
    - Bezug zur Unternehmensstrategie: Welche Bedrohungen von Erfolgsfaktoren und Risikotoleranz sind vorhanden?
    - Erfassung unsicherer Planannahmen aus Controlling und Planung
    - Auswertung von Planabweichungen zur Risikoidentifikation
3. Risikoanalyse und -quantifizierung:
    - Die verschiedenen Bewertungsskalen richten sich in Relation zur Organisation und ihrer Ziele, [pwc(2008), S.16].
    - Klare, überschneidungsfreie Abgrenzung von Risiken.
    - Abgrenzung von Risiken und sicheren Schäden.
    - Begründungen für die Risikobewertung dokumentiert.
    - Berücksichtigung der Wirkungsdauer von Risiken.
    - Quantitative Beschreibung der Risiken durch geeignete Wahrscheinlichkeitsverteilungen (z.B. Normal- oder Dreiecksverteilung).
    - Geeignetes Risikomaß (z.B. value-at-risk oder EUR) zur Priorisierung von Risiken.
    - Erfassung der Abhängigkeit zwischen wichtigen Risiken (Korrelationen) [2].

[2] Nur für fortschrittliche Risikomanagementsysteme möglich, es bedarf einen hohen Reifegrad in der Risikobeurteilung

Level:	1 Naiv bzw. Initial	2 Basis (Mindeststandard)	3 Standardisiert	4 Luxury
Ziele und Politik	Mündliche Festlegung von RM-Zielen und -Politik.	Schriftliche Festlegung inklusive Zeitplan.	RM-Ziele werden als Teil der ausformulierten Unternehmensziele erstellt.	Es bestehen mehrjährige Ziele für das RM und eine Strategie diese umzusetzen .
Kultur	Das Unternehmen ist sich ihrer Erfolgspotentiale und RM-Notwendigkeit nicht bewusst.	Potentieller Nutzen des RM ist kaum bewusst. Handlungen nur bei Bedarf.	Akzeptanz und klare Festlegung der Risikostrategie.	Gelebte und proaktive RM-Kultur. RM wird als Wettbewerbsvorteil gesehen.
Erfahrung	Keine Kenntnisse der Risikoprinzipien.	Erste Pilotprojekte im RM.	Ausgebildete interne Mitarbeiter.	RM wird in allen Bereichen angewandt.
Anwendung und Organisation	1. Kein strukturiertes Vorgehen für das Managen von Unsicherheiten. 2. Verantwortlichkeiten und Kompetenzen nicht klar verteilt.	1. RM Anwendungen haben keine Beständigkeit und nur Teilbereiche des RM sind mit Verantwortlichen geregelt. 2. Aus Bedrohungen werden in wichtigen Unternehmensbereichen Risiken identifiziert und bewertet.	1. Line of Defense - RM ist Bestandteil des operativen Geschäfts. 2. Line of Defense - Ein RM-Koordinator ist einer speziellen Abteilung zugewiesen. 3. Line of Defense - Interne Revision .	1. Eigene RM Organisationseinheit zum Kompetenzaufbau. 2. Keine Doppelgleisigkeiten- alle Abteilungen nutzen eine IT- Plattform . 3. Definierte Schnittstellen zu Prozessen der Steuerung und Abteilungen. 4. Regelmäßige RM Schulungen.
Risiko-orientiertes Prozessmanagement	1. Kaum Modellierung der wichtigsten Geschäftsprozesse. 2. Sporadisch formalisierte (schriftliche) oder strukturierte RM Anweisungen (Prozesse).	1. Basierend auf Geschäftsprozessen werden systematisch Risiken abgeleitet und bewertet. 2. Zur Verringerung dieser Risiken werden geeignete Kontrollmaßnahmen bestimmt.	1. Anwendung und Dokumentation von RM Prozessen und Kennzahlen auf Projekten. Risikoreduktion feststellbar. 2. Ausführliches Risikokontrollinventar inklusive Bewältigung und Verantwortlichen.	1. Risikobasierte Berichtgestaltung, Steuerung und Entscheidungsfindung. 2. RM Informationen werden aktiv genutzt (Frühwarnung, Performance, Kosten)
Compliance Management	Compliance Verständnis in den meisten Abteilungen nicht vorhanden.	Die relevanten Rechtsgebiete sind bekannt und werden zur Bewertung der Compliance Risiken herangezogen.	ident mit Level 2.	Compliance als etablierter und überwachter Bestandteil in den Prozessen. Regelmäßige Schulungen.
Interne Revision	Es wird überprüft ob die vorgesehenen Kontrollmaßnahmen eingehalten werden.	Risikoprüfinventar beinhaltet den Ablauf, Datum, Verantwortliche und Ergebnisse aller Prüfungen.	1. Überprüfung der RM Wirksamkeit. 2. Effektivitätsrisiken werden betreut .	Die interne Revision berichtet der Geschäftsführung im vollen Umfang über die Ergebnisse der Prüfung und diese werden umgesetzt.
Risiko-prozess: Identifikation	1. Wenige Einzelrisiken bzw. Risikoklassen werden überwacht. 2. Zentrale Erarbeitung von Risiken als top-down Prozess.	1. Umfangreicher top-down- oder/und bottom-up Prozess, z.B. mittels Expertenkomitee. 2. Risikoinventar (Einzelrisikokatalog).	1. Erarbeitung relevanter Risiken durch Experten, Fachquellen oder Mitarbeiter. 2. Ausführliches Risikoinventar (Segmentierte Kategorien) .	1. Umfassende Risikoklassifikation (Verknüpft Risiken mit z.B. Prozessen). 2. ganzjähriges RM für alle Mitarbeiter . 3. Risikoidentifikatoren dienen als Frühwarnsystem.
Bewertung	Quantitative oder qualitative Bewertung von Einzelrisiken in Form von Einschätzungen.	1. Fundierte Einzelrisikoanalysen. 2. Vereinfachte unternehmensweite Übersicht durch z.B. Risikomatrix. 3. Risikohöhe zumindest qualitativ geschätzt .	1. Umfassende Bewertung mittels Risikokennzahl. 2. Bevorzugung von quantitativen Methoden und Nachvollziehbarkeit bei nicht quantifizierbaren Risiken. 3. Analyse der Wechselwirkungen von wesentlichen Toprisiken. 4. Erste Aggregationsversuche.	1. Risikoaggregation (für Simulation und Stresstests). 2. Korrelations-/Sensitivität Analysen, Analyse möglicher Dominoeffekte und Querschnitts-Themen. 3. Verlustdatenbank der eigenen bzw. branchenüblichen Verluste und Historie.
Steuerung	Beobachtung der Risikoentwicklung auf IST-Basis (wesentliche Veränderungen sind ausschlaggebend für Handlungen).	1. Risiken haben entsprechende Steuerungsmaßnahmen. 2. Priorisierung, durch Definition von zur Zeit aktuellen Toprisiken .	1. Risikokennzahlen beeinflussen die Maßnahmenfülle und deren Priorität. 2. Festlegung von Zielwerten, Toleranzgrenzen/Schwellwerten.	RM als integrierter Bestandteil der Unternehmenssteuerung und der dazugehörenden Informationssysteme.
Reporting	Einhaltung der gesetzlichen Berichtsstruktur.	Berichte sind anlassbezogen, manche bereits strukturiert erstellt.	Standardisierte interne Berichtsstruktur bezüglich Inhalt, Tiefe und Detailierungsgrad.	1. automatisierbare Ad-hoc-Berichte. 2. Informationssystem vorhanden mit dashboards bzw. activity-monitoring.

Tabelle 4.3: Reifegrade im industriellen Risikomanagement [Schleinzer(2014), vgl. Abb. 30]

4. Risikoaggregation:

   - Aggregation statt Addition der wichtigsten Risiken und deren genaue Unterscheidung!
   - Aggregation von Einzelrisiken mit Bezug zur Unternehmensplanung (Monte-Carlo-Simulation).
   - Berechnung des Gesamtrisikoumfangs (Eigenkapitalbedarf) bzw. Bezug zum Rating und zur Finanzierungsplanung.
   - Management benötigt Aggregation in Form einer Portfolioansicht der Risiken um ihnen als Entscheidungsgrundlage zur Risikobewältigung zu dienen, [pwc(2008), S.18].
   - Verbindungen und Abhängigkeiten (Kaskaden- und Kumulativwirkungen) zwischen den Risiken und gegenüber Maßnahmen beachten [ISO(2009), S.26].
   - Definition eines risikoorientierten Erfolgsmaßstabs (Performancemaß), z.B. RORAC [3].

5. Risikobewältigung:

   - Betrachtung unterschiedlicher Risikobewältigungsmaßnahmen gegenüber verschieden Risiken.
   - Abgrenzung von Kern- und Randrisiken.
   - Ein Risikobewältigungsplan ist eine Methode des Projektmanagements, um Übersicht über Prioritäten und alle Maßnahmen zu behalten [ISO(2009), S.29].
   - (Quantitative) Frühaufklärungssysteme und Prognosesysteme.
   - Abwägung von Risiken und Ertrag bei Entscheidungen (z. B. bei Investitionen).
   - Ermittlung der Restrisiken (Bedeutung und Häufigkeit), [pwc(2008), S.15] .

6. Risikokontrolle:

   - Mittels Risikokennzahlen (engl. KPI) und Frühindikatoren werden potentielle Risiken kontrolliert [pwc(2008), S.19].

7. Risikoüberwachung und Gestaltung des Risikomanagementsystems:

   - Schwerpunktsetzung bei wichtigen Risiken zur Vermeidung bürokratischen Aufwands.
   - Verbindung mit bestehenden Organisations-, Planungs-, und Berichtssystemen (insb. Controlling, BSC, QMS).
   - Vollständige und verständliche Dokumentation der Prozesse im Risikomanagement, gegebenenfalls IT-gestützt.

[3] Die beiden letzten Aufzählungspunkte sind nur für fortschrittliche Risikomanagementsysteme nötig

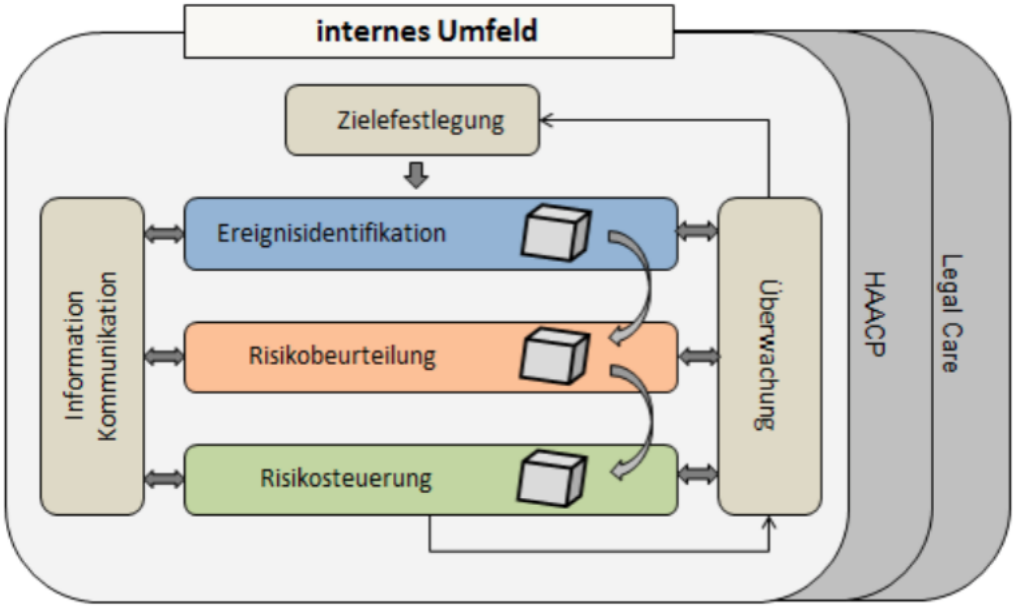


Abbildung 4.4: Beispielhafter Risikomanagementprozess eines mittelständischen Lebensmittelkonzerns mittels COSO II nach Christoph Aichinger

- Klare Aufgabenzuordnung im Risikomanagement, insbesondere zur Risikoüberwachung.
- Benennung eines Verantwortlichen für das Gesamtsystem.
- Organisatorische Trennung zwischen Risikomanagement und interner Revision.
- Einbindung der Mitarbeiter ins Risikomanagement und Risikokultur.
- Festlegen von Risikopolitik und Limitsystem sowie Risikoreporting.

Bei jedem Prozessschritt stehen wie in der oberen Aufzählung gezeigt, mehrere Methoden zur Auswahl. Letztendlich liegt es zu einem gewissen Grad an dem Risikomanager und -eigner welche ihnen am sinnvollsten und lösungsorientiertesten erscheint.

Die Darstellung des konzerneigenen Risikomanagementprozesses ist bestenfalls, ähnlich Abbildung 4.4, zu skizzieren und auf konzerneigene Veränderung gegenüber dem Standardmodell in Abschnitt 2.2 ist einzugehen. In Anlehnung an den COSO II ERM-Würfel wird jedes Risiko mit den drei Risikomanagement Dimensionen: Organisationseinheit, Risikokategorien und Prozessstufen verbunden.

Die Abbildung 4.5 zeigt einen beispielhaften jährlichen Risikoprozess als Fließdiagramm inklusive schrittweiser Aufgabenabfolge und Verantwortlichkeiten. Natürlich gibt es noch weitere Varianten von Risikomanagementprozessen, beispielsweise Schwaigers Regelkreis gesteuerten Risikomanagementprozess [Schwaiger(2013), Folie 10ff.].

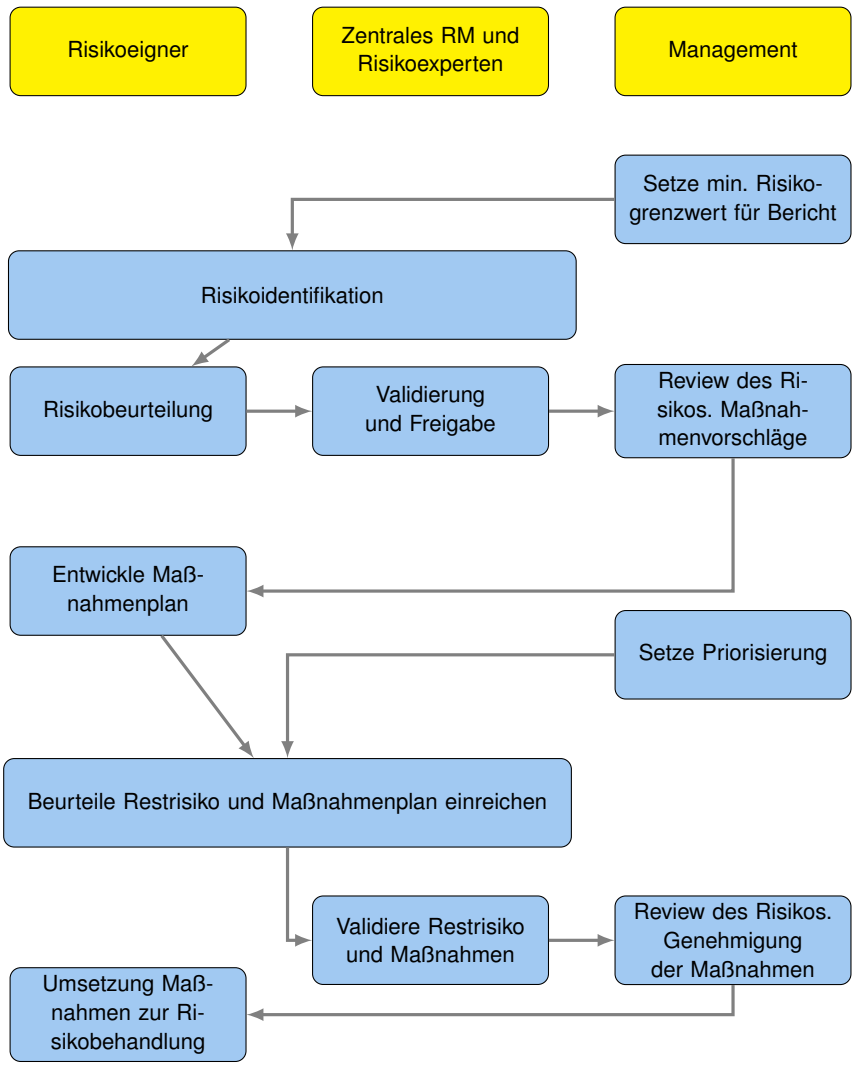


Abbildung 4.5: Beispiel für einen jährlichen Risikomanagementprozess inklusive Verankerung in die Organisation [Popescu(2014), F. 24]

Verpflichtende Methoden für den konzerneigenen Risikomanagementprozess

Die hier angeführten Methoden sind im Detail in Abschnitt 3.6, Abschnitt 3.7, Abschnitt 3.8 und Abschnitt 3.9 beschrieben und könnten genau so als Textpassagen auch in ein Risikomanagementhandbuch eingefügt werden.

Der Konzern orientiert sich in seinem initialen Einführungsprozess an den sehr übersichtlichen Methoden in **[Curtis and Carey(2012)] Methoden**. Die folgenden Methoden dienen dem Konzern als Mindeststandard:

- Risikoidentifikation und -analyse mittels konzernweiten und moderierten Expertenworkshops (aus dem engl. facilited-workshops), siehe Abschnitt 3.6.
- Datenanalyse und -kategorisierung innerhalb des Risikomanagement Projektteams, siehe Abschnitt 3.6, Abschnitt 4.5 und Abschnitt 4.8.
- Risikobeurteilung mittels Risikolandkarten und qualitativer Expertenschätzung der Risikohöhe, siehe Abschnitt 3.7 und Abschnitt 4.5.
- Das VaR (value-at-risk) als normalverteiltes Risikomaß kann im Konzern nur bei den Finanzrisiken eingesetzt werden. Zur Berechnung wird der Wert der dem 95%-Perzentil am nächsten kommt aus der vorhandenen Zahlenreihe als mögliche VaR-Risikohöhe herangenommen. Ein Beispiel: Bei einer Datenreihe der letzten 100 eingetretenen Verluste durch Kundeninsolvenzen, wäre der 95. Wert gleich dem 95%-VaR. Details siehe Abschnitt 3.7.
- Eine Risikomatrix wird sowohl als Visualisierung einzelner Risiken Abbildung 4.9 verwendet als auch zur Risikoaggregation (Portfolioansicht) für mehrere Risiken nach Abbildung 4.10.
- Ein elektronischer Fragebogen zur regelmäßigen Evaluierung dient künftig zur regelmäßigen Aktualisierung der Risikosituation siehe Abbildung 4.16.
- Die Steuerung der Maßnahmen erfolgt dem Projektmanagement folgend mittels Maßnahmenplan, siehe Abbildung 4.13, Abbildung 4.12 und Tabelle 3.5.
- Ein konzerneigener Risikokontenplan schlüsselt mit einer Nummerierungslogik ähnlich zur Finanzbuchhaltung eindeutig die Art des Risikos und deren lokale Verantwortlichkeit (Abteilung, Gesellschaft und Standort) auf. Dies stellt, bei der Fülle an Risiken, einen wesentlichen Übersichtsgewinn bei der Steuerung dar, siehe Abschnitt 4.5.
- Die Festlegung der externen und internen Berichterstattungsprozesse ist anhand der Rollenzuteilungen in Abbildung 4.2 im Informationssystem möglich und mittels Rollenkategorien auch übersichtlich.
- Die Kontrolle erfolgt über Ansichten im Informationssystem (engl. dashboards), welche nach Dimensionen wie Periode, Organisationseinheit, Risikokategorie oder Verantwortlichkeit gefiltert dargestellt werden können. Das Dashboard verwendet tabel-

larische Auflistungen aller Maßnahmen und Visualisierung mittels Risikomatrix, siehe Abbildung 4.15.

- IT-unterstützte Risikostammblätter dienen dem kompletten Risikomanagementprozess ähnlich einem Formular bei der Risikomanagementkommunikation, -dokumentation, -berichterstattung, -kontrolle, -beurteilung und -steuerung. Die schlichteste Form eines Risikostammblattes wird in Abbildung 6.4 gezeigt.

Der komplette Risikomanagementprozess im Konzern ist mittels IT-Plattform abgebildet, Details sind in Kapitel 6 geschildert. Anhand der Benutzeroberfläche dieser Softwarelösung, werden auch die einzelnen Prozessschritte in den folgenden Unterkapiteln schrittweise aufgebaut und erklärt.

IT-unterstützte Risikostammblätter als Kommunikationsgrundlage des Prozesses

Das Konzept des Risikostammblatts nach Abschnitt 3.10 ist die zentrale Informationseingabe und -präsentation für alle im Risikomanagement beteiligten Personen. Nach jedem Schritt im Risikomanagementprozess werden dort die Ergebnisse eingetragen, verlinkt, versioniert und freigegeben.

Die Abbildung 6.4 zeigt eine schlichte Form des Risikostammblatts. Die Abbildungen im folgenden Kapitel zeigen oftmals Screenshots aus dem eigens entwickelten Prototypen mittels der business-intelligence Softwareplattform prevero p750 (maple leaf).

Zieldefinition

Die Ziele und Leitbilder eines Konzerns werden in der Geschäftsführung getroffen und müssen von internen Dokumenten entnommen werden. Allgemeine Details zur theoretischen Zielfindung oder Ziele des Risikomanagement findet man in Abschnitt 3.3.

Als Zieldefinition bei den einzelnen Risikoklassen im Unternehmen eignet sich folgendes Beispiel, wobei ein ○ niedriger, ◐ mittlerer und ◐ hoher Risikoappetit bedeutet:

Risikoidentifikation durch geführte Expertenworkshops

Die bottom-up Methode mittels Workshops wurde für unseren Konzern als die langfristig erfolgsversprechende identifiziert, siehe Abschnitt 3.4 und Abschnitt 3.6

Die **Identifikation** der konzerneigenen Risiken dienen der Beantwortung der folgenden Fragestellungen:

- Was kann wo und wann passieren? Die Suche nach einer möglichst kompletten Auflistung von jenen Ereignissen die den Unternehmenszielen entgegenwirken und deren Zusammenhänge.
- Warum und wie können Ereignisse passieren? Nachdem Ereignisse im ersten Schritt identifiziert wurden, werden im zweiten Schritt deren Quellen und Lösungsmöglichkeiten identifiziert.

Risikoarten	Gesamt	Verkauf	Organisation	Tochtergesellschaft
Kreditrisiken	◐	◐	◐	○
Marktrisiken	◐	◐	○	○
Operative Risiken	◐	○	●	◐
Geschäftsrisiken	◐	●	○	○

Tabelle 4.4: Beispielhafter Risikoappetit nach Risikokategorien nach [Stegemann(Februar 2014), vgl. Exhibit 5].

- Wer ist betroffen und involviert? Dies kann alle Stakeholder innerhalb und außerhalb des Unternehmens beinhalten.

Nach dem in Abschnitt 4.3 beschriebenen Subsidiaritätsprinzip sind Risikoeigner für die in ihren Bereich entstehenden Risiken auch verantwortlich. Dem normgerechten Risikomanagementprozess folgend muss dieser Abschnitt jedoch mindestens neue Risiken des laufenden Geschäftsfeldes identifizieren und bestehende Risiken regelmäßig evaluieren, ob sie noch in derselben Höhe vorhanden sind. Mögliche Methoden sind im eigenermessen des Risikoeigners zu wählen und können z.B. Befragungen von Experten, Fachliteratur oder die Beobachtung des Marktumfeldes beinhalten.

Die Umsetzung des Identifikationsschrittes mittels Software ist in Abbildung 4.6 zu sehen, indem in der angegebenen Ansicht Risiken gesucht werden können und sich eine Auflistung mit Detailinfos automatisch öffnet. Weitere Erläuterungen:

- Das Abbildung 4.7 wiederum zeigt die Eingabe von neuen Risiken, nachdem diese ergebnislos in (Abbildung 4.6) gesucht wurden und es keine Vorversion gibt.
- Die grau unterlegten Felder sind vom administrierenden Risikomanager bzw. -experten vorgegeben und die weißen Felder sind die Eingabe- bzw. Auswahlfelder des Risikoeigners. Die grauen Felder sind für Vorgaben zur Skala, Einheiten, Verantwortlichen, Datum, Versionen, der Bewertungsmethode, Zuteilung der Risikokategorie oder andere Stammdaten reserviert.

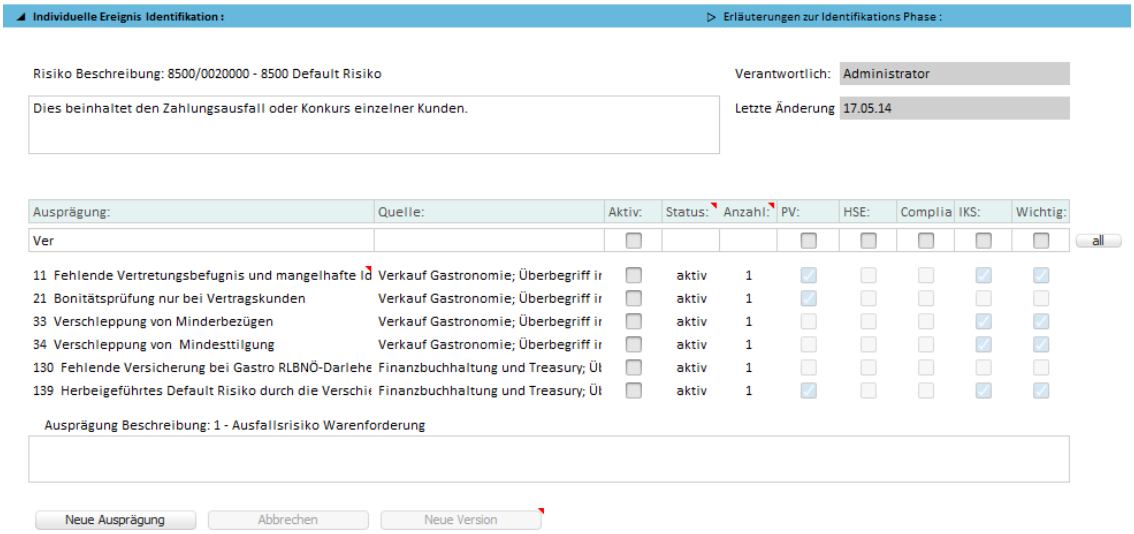


Abbildung 4.6: Prototypische Umsetzung der Ansicht und Suche von Risiken

- Die sogenannten “individuellen Ereignisse” (hier als negative Risiken auftretend) sind Risiken die bereits einer Kategorie und Eigenschaften zugeteilt wurden, aber im Unternehmen häufiger vorkommen, wie in Abschnitt 4.5 geschildert. Jedem betroffenen Risikoeigner wird also nach Abbildung 4.14 ein eigenes “individuelles Ereignis” vom gleichen Ereignis zugeteilt und somit auch ein eigenes Stammblatt Abbildung 6.4. So kann es leicht passieren dass ein Dutzend Risikoeigner ein leicht abweichendes individuelles Risiko namens Arbeitssicherheit oder Kreditausfall tragen.

- Bei der Arbeitssicherheit in den Bereichen wie Logistik, Produktion oder Außendienst treten unterschiedliche Ausprägungen auf. Ein Risikoeigner muss diese unterschiedlich bewerten oder behandeln, wie in Abbildung 4.7 ersichtlich. Dafür dient die eigene Dimension “Ausprägung”, bei der es sich um spezielle Risikoeigenschaften beim jeweiligen individuellen Ereignis handelt. Die Ausprägungen sind in einer eigenen Datenbank und können vom Risikoeigner gesucht, hinzugefügt, entfernt, variiert oder versioniert werden, alles dokumentiert und prozesskonform.

- Die ausgewählten Pflichtfelder (mit *) generieren automatisch eine Risikokontonummer (siehe Abschnitt 4.5) und legen die Datenbankeinträge an.

- Weitere Eingabemöglichkeiten dienen der effizienten Sortierung und Sonderbehandlung, wie hier durch abhacken von relevanten Themen gezeigt, insbesondere Arbeitssicherheit, Compliance, Detailanalyse wegen Komplexitätshöhe, Zusatzkontrollen oder zu erwartende Priorität als Toprisiko.

- Beschreibungen sind freie Textfelder die zur Erläuterung der oft nur kurzgefassten Bezeichnungen dienen sollen. Dabei beschreibt der Risikoeigner den für ihn klaren

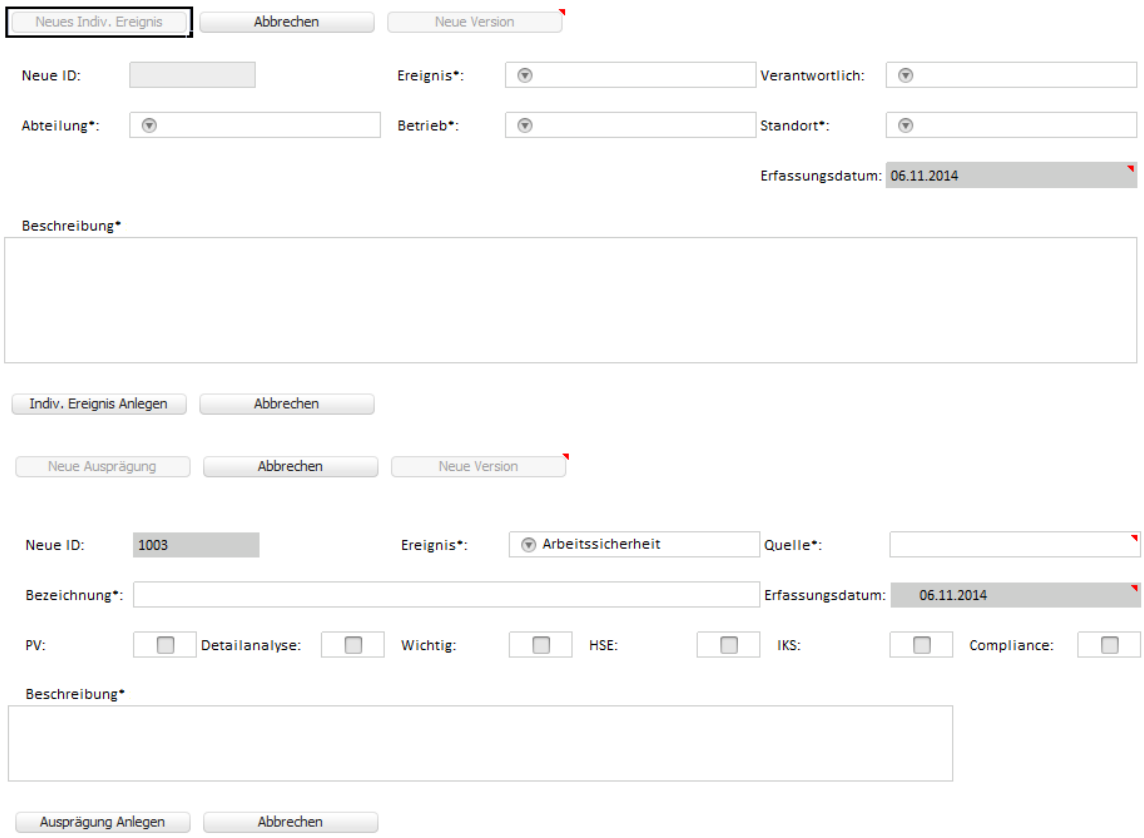


Abbildung 4.7: Prototypische Umsetzung der Eingabe von Risiken

Sachverhalt für Dritte.

Risikoanalyse mittels Einteilung in Risikokategorien

Die Risikokategorien dienen dazu, einen Überbegriff für mehrere ähnliche Risiken und deren Risikomodelle (Vorhersagen, Detailanalysen, Maßnahmen) zu schaffen, um die Weiterarbeit an ähnlichen Themenstellungen zu erleichtern. Anhand dieser Kategorien können automatisiert weitere wichtige Einteilungen zu den beinhalteten Risiken zugeteilt werden. Beispielsweise die in interne/externe Risiken, in systemimmanente Risiken (jene die nicht/kaum durch Maßnahmen verbessert werden können, z.B. Branchenrisiken) und Restrisiken (welche veränderbar sind).

Folgende Fragestellungen dienen als Anhaltspunkt:

- Welche vorhandenen Systeme, Prozesse oder Hilfsmittel können Ereignisse verhindern, aufspüren oder verringern. Sowohl deren Bedeutung als auch deren Häufigkeit?

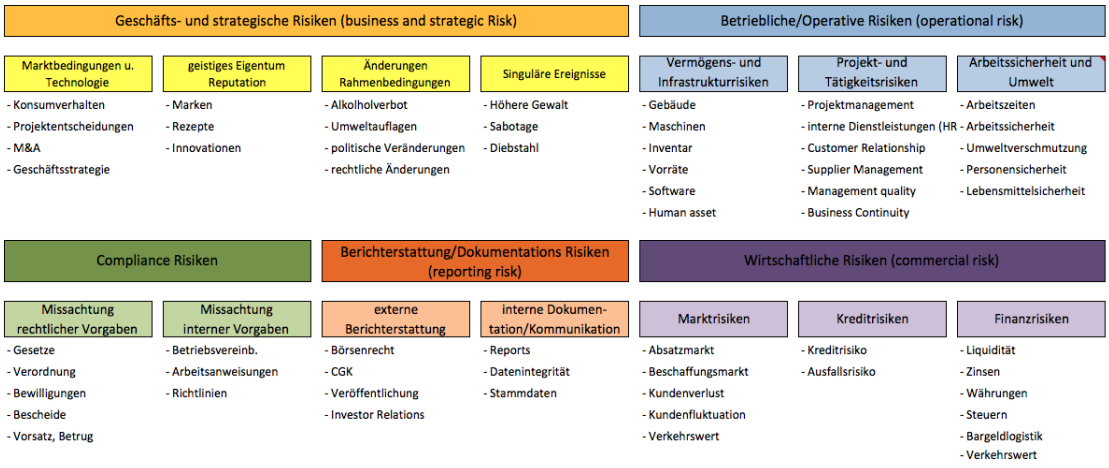


Abbildung 4.8: Unterteilung der Risiken in Kategorien [Olsen et al.(2011)Olsen, Plaschke, and Stelter, vgl. Exhibit 3], Graphik Christoph Aichinger

- Wie sicher können sie sich ihrer Bewertung und der zugrunde liegenden Datenquellen sein? Wie genau verstehen sie die zugrunde liegenden Unsicherheiten und Wahrscheinlichkeiten?

- Dort wo die höchsten Unsicherheiten bezüglich der Bewertungsergebnisse mit den größten Bedeutungen oder Häufigkeiten einhergehen, müssen weiterführende Detailanalysen stattfinden.

Die Abbildung Abbildung 4.8 zeigt die im Konzern verwendeten 5 Risikokategorien, deren Entstehung näher in Abschnitt 3.6 erläutert wird. Diese Kategorien werden in weiterer Folge in allen Schritten des Risikomanagementprozesses und im Informationssystem verwendet. Sie schaffen zusammen mit dem Risikokontenplan Abschnitt 4.5 eine Übersichtlichkeit, denn statt hunderter oft ähnlicher Risiken werden dann nur einige dutzend breiter gefasste Risikokategorien behandelt.

Risikobeurteilung und Aggregation mittels Risikolandkarten

Die Risikobeurteilung setzt sich aus Analyse und Bewertung zusammen. Sie wird mindestens mittels qualitativer Expertenschätzung nach ONR49002-2 [ONR(2014d), Tabelle A.1] abgehalten und erhält je nach Anwendungsfall angepasste Risikokriterien und -skalen. So oft wie das die vorhanden Informationen ermöglichen, sollen quantitative Schätzungen getätigt werden. In Abbildung 4.9 erfolgt die Beurteilung mittels Risikolandkarten (auch Risikomatrix genannt) und kann durch die Auswahl der Skalen sowohl in quantitativer als auch qualitativer Form erfolgen.

Die **Beurteilung** setzt sich aus Analyse und Bewertung zusammen. Dies beinhaltet zumindest folgende Tätigkeiten:

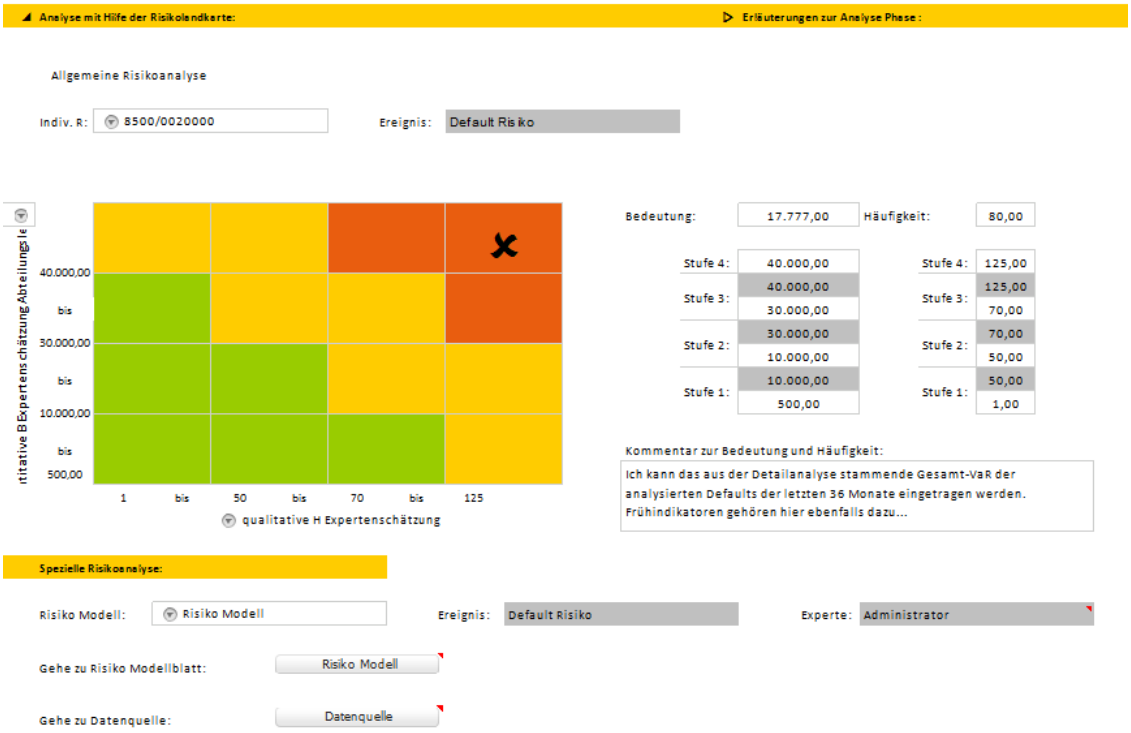


Abbildung 4.9: Prototypische Umsetzung der Beurteilung von Risiken

- Bewertung der Häufigkeit und Bedeutung des eintretenden Risikos.
- Gruppierung der Risiken in Risikokategorien
- Bei Verfügbarkeit von historischen Daten Ermittlung von quantifizierten Risikohöhen
- Selektion der Toprisiken und Darstellung mittels Risikomatrix
- Bewertung des verkraftbaren Risikos mittels einer Gegenüberstellung der Unternehmensziele

Abbildung 4.9 zeigt eine beispielhafte Umsetzung der IT-unterstützten Bewertung. Dabei sind die grau unterlegten Felder vom administrierenden Risikomanager bzw. -experten vorgegeben und die weißen Felder dienen als Eingabefelder. Die grauen Felder enthalten Vorgaben zur Skala, der Bewertungsmethode, Zuteilung der Risikokategorie oder Stammdaten. Sie sind nur über einen dokumentierten Änderungsprozess veränderbar und dienen einer unternehmensweiten Standardisierung die sowohl zur Aggregierung, gemeinsamen Sprache und einheitlichen Prozessrichtlinien notwendig ist. Weiterführende Links geben die Möglichkeit detaillierte Risikoberechnungen durchzuführen (z.B. VaR oder Monte-Carlo-Simulation) und die risikospezifischen Datenquellen einzusehen. Schließlich können in je-

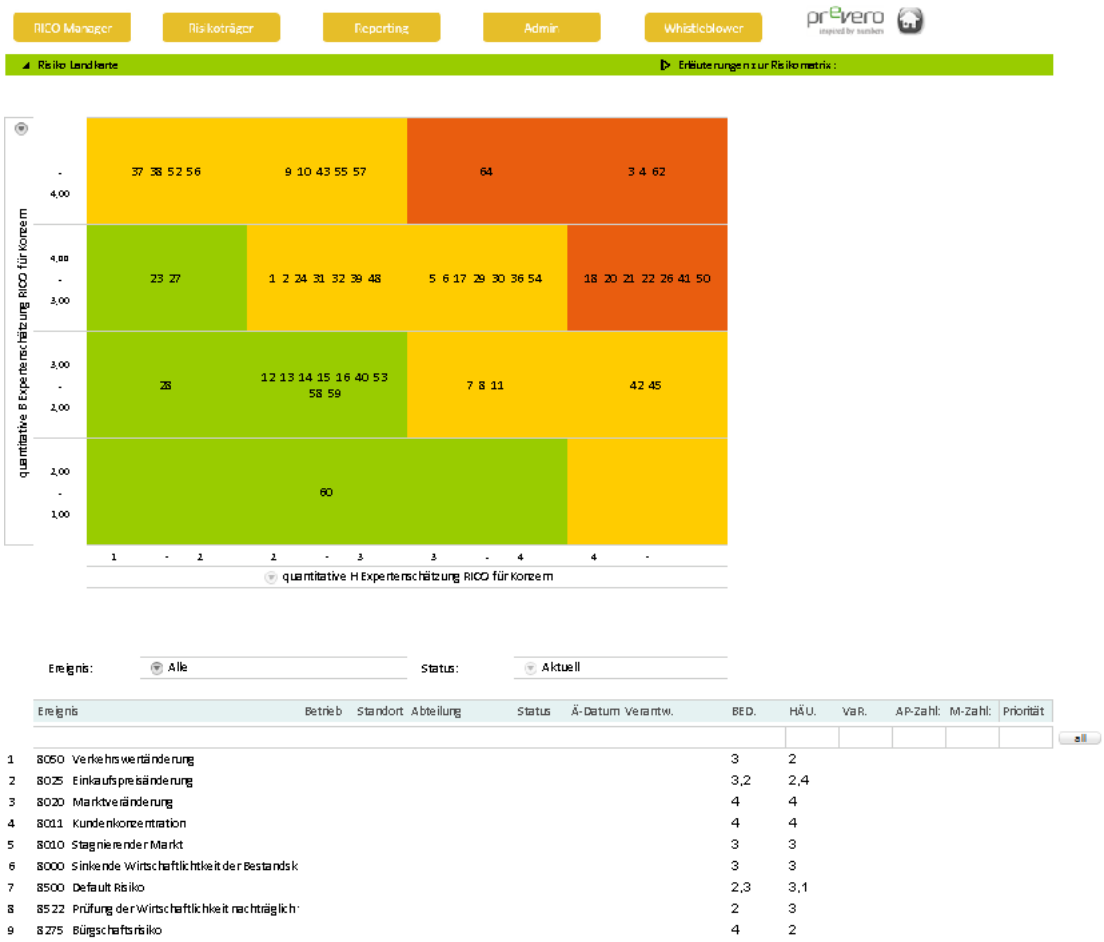


Abbildung 4.10: Prototypische Umsetzung der Portfolioansicht von Risiken

dem Schritt Kommentare gesetzt werden, als Erinnerung, Dokumentation und Diskurs mit anderen Teilnehmern.

Die Aggregierung von Risiken meint zwei Punkte, die gegenseitige Beeinflussung von Risiken in Form von Korrelationen und das Ergebnis einer Zusammenführung von Einzelrisiken. Die Zusammenführung von Einzelrisiken kann unterschiedlich in der gängigen Praxis erfolgen. Die im Konzern umgesetzte Aggregierung erfolgt durch Risikolandkarten, die eine Zusammenfassung oder Filterung von Hierarchieebenen, Verantwortlichen, Ländern, Unternehmensbereichen oder Risikokategorien bewerkstelligen. Die Auswertung der 16 Felder innerhalb der Risikolandkarte und eine erneute Expertenschätzung dient als Ermittlung der Toprisiken für die Geschäftsleitung.

Die Risikolandkarte und erneute Expertenschätzung ist die einfachste Form der Aggregierung in der Praxis, siehe Abbildung 4.10. Die Begründungen für ihre Verwendung liegen darin, dass die Berechnung von Korrelationen, Datenreichtum von dem untersuchten Risiko

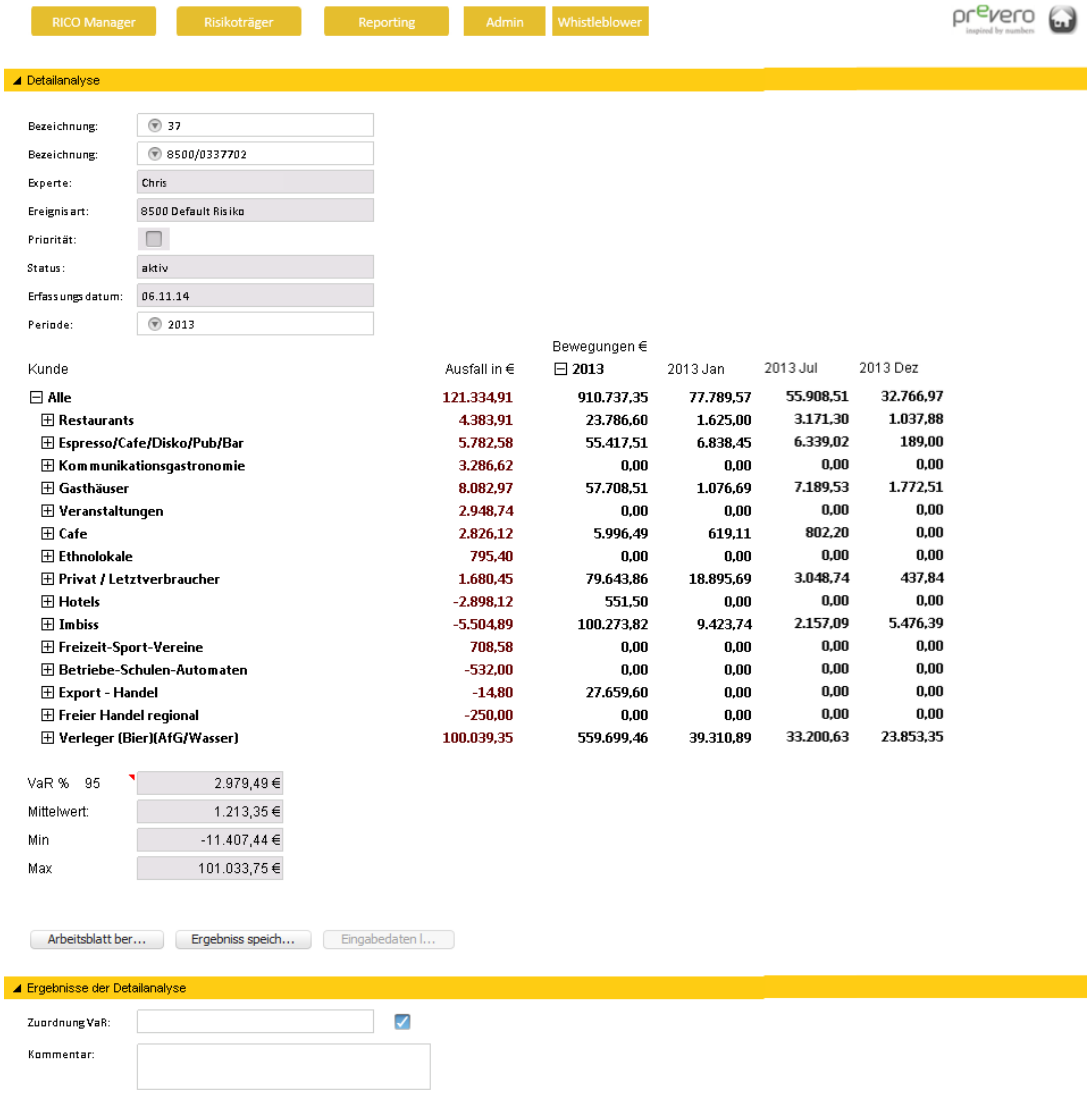


Abbildung 4.11: Prototypische Umsetzung der Detailanalyse von Ausfallrisiken

verlangt, dies ist in den seltensten Fällen gegeben. Alle ausgereifteren Formen der Aggregierung bedürfen Korrelationen. Die Aggregierung in all ihren Facetten ist ein aktuelles Forschungsgebiet und wird erst in künftigen Ausbauschritten erweitert werden.

In Abbildung 4.11 wird für die Detailanalyse der Ausfallrisiken beispielhaft ein eigenes Arbeitsblatt gestaltet.

Steuerung bzw. Bewältigung

Die **Steuerung** befasst sich mit der Bewältigung oder Übertragung der Risiken, kurz deren Lösung bzw. Handhabung. Die Aufgaben umfassen den Maßnahmenplan bzw. Risikobewältigungsplan mit Verantwortlichkeiten, Terminen, Kosten, betroffenen Bereichen und Restrisiko. Eine dem Projektmanagement ähnliche Herangehensweise wird empfohlen. Die Steuerung bedarf eines Überblicks durch Portfolioansichten wie in Abbildung 4.10 gezeigt und setzt darauf aufbauend Prioritäten und Kontrollen.

- Während dieses Prozessschrittes werden die in der Risikoanalyse ermittelten Risikowerte mit den Risikokriterien aus den Unternehmenszielen verglichen und dementsprechend besteht Handlungsbedarf.
- Die Bewältigung beinhaltet die Ermittlung der möglichen Optionen in Form von Maßnahmen, sowie deren Auswahl und Umsetzung mittels Maßnahmeplänen. Es verbleibt ein Restrisiko.
- Im Spannungsfeld zwischen Kosten und Nutzen muss zwischen reduzierenden (Bedeutung oder Häufigkeit), versichernden, verlagernden oder verhindernden Maßnahmen gewählt werden.

Risikosteuerung mittels projektgesteuerten Maßnahmeplänen

In Abbildung 4.12 erfolgt die Steuerung der Risiken durch Eingabe und Auswahl von Maßnahmen als Teilschritt des Risikomanagementprozesses (bzw. diesen repräsentierenden Risikostammblatts). Bestehende Maßnahmen können gefiltert, zugeteilt oder abgebrochen werden.

Die Maßnahmen können in der Projektmanagement Ansicht in Abbildung 4.13 permanent gesteuert werden. Informationen zu den Deadlines, Budgetstatus, Maßnahmenfortschritt oder Verantwortlichen sind hier übersichtlich aufgelistet.

Risikosteuerung mittels Risikokontenplan

Im Zuge des, in dieser Arbeit vollzogenen, Praxisprojekts wurde die Idee eines Risikokontenplans entwickelt. Die dutzenden Risikokategorien nach Abbildung 4.8 können mittels Risikokontenplan und den darin verwendeten Zifferncode übersichtlich auf die Verantwortlichen und Unternehmensbereiche verteilt werden. Gleichzeitig kann mit dem Zifferncode sowohl einfach übergeordnet aggregiert als auch gemeinsam mit Experten unternehmensübergreifend diskutiert und verbessert werden.

Begründet liegt der Bedarf dieses überschaubaren Ordnungssystems, vor allem in der Natur der Risiken selbst, die überall im Unternehmen mehrfach, asynchron in zufälliger Reihung oder synchron mit gegenseitiger Abhängigkeit auftreten können. Wie im beispielhaften Organigramm Abbildung 4.14 gezeigt, tritt das Kreditausfallrisiko in einem Konzern in mehreren Bereichen und Tochterunternehmen auf, in diesem Fall acht mal in 2 Betrieben und 3 Werksstandorten. Wird nun das Risiko dezentral (bottom-up) im Unternehmen behandelt,

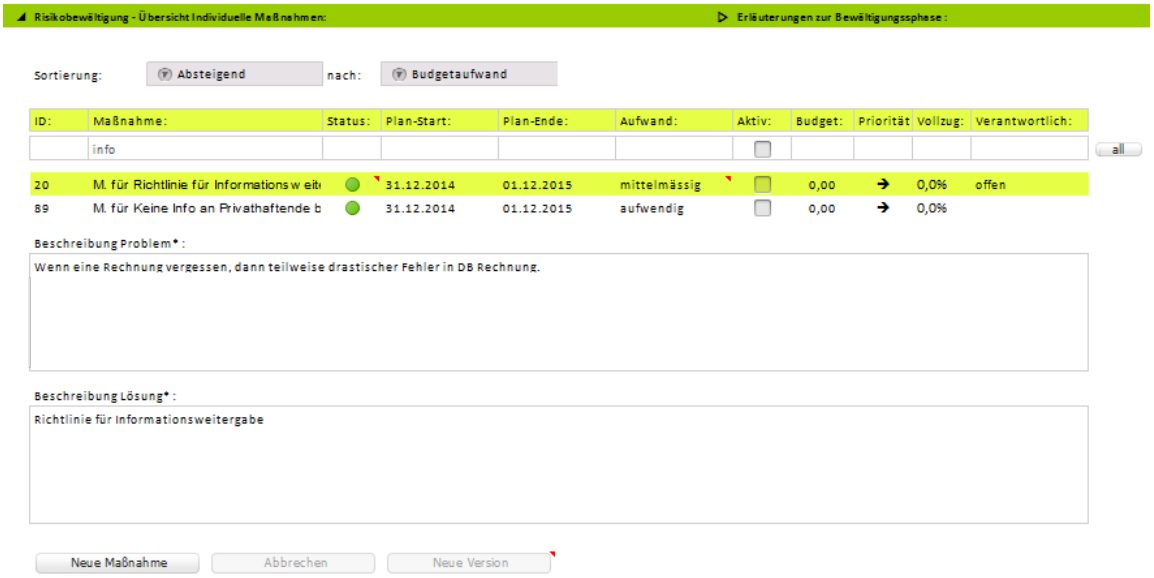
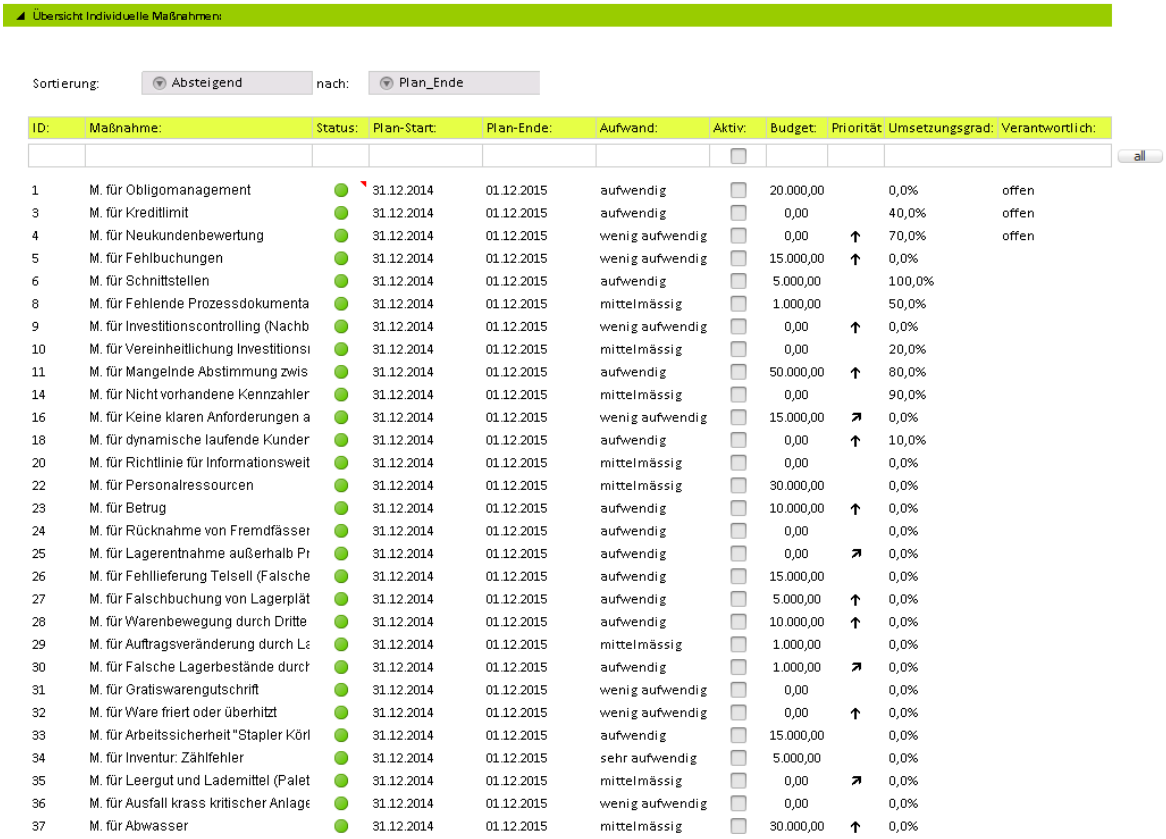


Abbildung 4.12: Prototypische Umsetzung der Steuerung von Risiken

sind auch mehrere Risikoeigener verantwortlich. Dabei ist es möglich, dass es in verschieden Abteilungen oder Risikoeignern auch verschiedene Ausprägungen eines Risikos gibt und es somit andere Maßnahmen bedürfen! Das Kreditausfallrisiko ist keine Ausnahme sondern die Regel! Die meisten Risikokategorien treten in einem Unternehmen mehrfach in verschiedenen Abteilungen, abgewandelt in der gleichen Abteilung oder abgewandelt in verschiedenen Abteilungen auf. Den Ansatz einzelne Risikokategorien nur einem Verantwortlichen zu überlassen und unternehmensweit (top-down) zu behandeln, wird wegen der fehlenden Praxisnähe und -tauglichkeit im Konzern nicht verfolgt.

Der Risikokonten Plan erleichtert die tägliche Arbeit mit langen Risikoinventurlisten und Risikostammblättern.

Folgende Tabelle 4.5 zeigt eine Nummerierungslogik für das Risikomanagement mittels neuentwickelten Risikokonten Plan. Die Bezeichnungen der Betriebe, Standorte und Abteilungen sind der aktuellen Kostenstellen-Nummerierung der Finanzbuchhaltung entnommen. Das Ereignis ist nach Risikokategorie in von 1 bis 9999 nummeriert, siehe Tabelle 4.6.



Übersicht Individuelle Maßnahmen:

Sortierung: Absteigend nach: Plan_Ende

ID:	Maßnahme:	Status:	Plan-Start:	Plan-Ende:	Aufwand:	Aktiv:	Budget:	Priorität	Umsetzungsgrad:	Verantwortlich:
										all
1	M. für Obligomanagement		31.12.2014	01.12.2015	aufwendig		20.000,00		0,0%	offen
3	M. für Kreditlimit		31.12.2014	01.12.2015	aufwendig		0,00		40,0%	offen
4	M. für Neukundenbewertung		31.12.2014	01.12.2015	wenig aufwendig		0,00	↑	70,0%	offen
5	M. für Fehlbuchungen		31.12.2014	01.12.2015	wenig aufwendig		15.000,00	↑	0,0%	
6	M. für Schnittstellen		31.12.2014	01.12.2015	aufwendig		5.000,00		100,0%	
8	M. für Fehlende Prozessdokumenta		31.12.2014	01.12.2015	mittelmässig		1.000,00		50,0%	
9	M. für Investitionscontrolling (Nachb		31.12.2014	01.12.2015	wenig aufwendig		0,00	↑	0,0%	
10	M. für Vereinheitlichung Investitionsı		31.12.2014	01.12.2015	mittelmässig		0,00		20,0%	
11	M. für Mangelnde Abstimmung zwis		31.12.2014	01.12.2015	aufwendig		50.000,00	↑	80,0%	
14	M. für Nicht vorhandene Kennzahler		31.12.2014	01.12.2015	mittelmässig		0,00		90,0%	
16	M. für Keine klaren Anforderungen a		31.12.2014	01.12.2015	wenig aufwendig		15.000,00	↗	0,0%	
18	M. für dynamische laufende Kunder		31.12.2014	01.12.2015	aufwendig		0,00	↑	10,0%	
20	M. für Richtlinie für Informationsweit		31.12.2014	01.12.2015	mittelmässig		0,00		0,0%	
22	M. für Personalressourcen		31.12.2014	01.12.2015	mittelmässig		30.000,00		0,0%	
23	M. für Betrug		31.12.2014	01.12.2015	aufwendig		10.000,00	↑	0,0%	
24	M. für Rücknahme von Fremdfässer		31.12.2014	01.12.2015	aufwendig		0,00		0,0%	
25	M. für Lagerentnahme außerhalb Pr		31.12.2014	01.12.2015	aufwendig		0,00	↗	0,0%	
26	M. für Fehllieferung Telsell (Falsche		31.12.2014	01.12.2015	aufwendig		15.000,00		0,0%	
27	M. für Falschbuchung von Lagerplät		31.12.2014	01.12.2015	aufwendig		5.000,00	↑	0,0%	
28	M. für Warenbewegung durch Dritte		31.12.2014	01.12.2015	aufwendig		10.000,00	↑	0,0%	
29	M. für Auftragsveränderung durch La		31.12.2014	01.12.2015	mittelmässig		1.000,00		0,0%	
30	M. für Falsche Lagerbestände durch		31.12.2014	01.12.2015	aufwendig		1.000,00	↗	0,0%	
31	M. für Gratiswarengutschrift		31.12.2014	01.12.2015	wenig aufwendig		0,00		0,0%	
32	M. für Ware friert oder überhitzt		31.12.2014	01.12.2015	wenig aufwendig		0,00	↑	0,0%	
33	M. für Arbeitssicherheit "Stapler Körl		31.12.2014	01.12.2015	aufwendig		15.000,00		0,0%	
34	M. für Inventur: Zählfehler		31.12.2014	01.12.2015	sehr aufwendig		5.000,00		0,0%	
35	M. für Leergut und Lademittel (Palet		31.12.2014	01.12.2015	mittelmässig		0,00	↗	0,0%	
36	M. für Ausfall krass kritischer Anlage		31.12.2014	01.12.2015	wenig aufwendig		0,00		0,0%	
37	M. für Abwasser		31.12.2014	01.12.2015	mittelmässig		30.000,00	↑	0,0%	

Abbildung 4.13: Prototypische Umsetzung des Maßnahmenplans und dessen Verwaltung

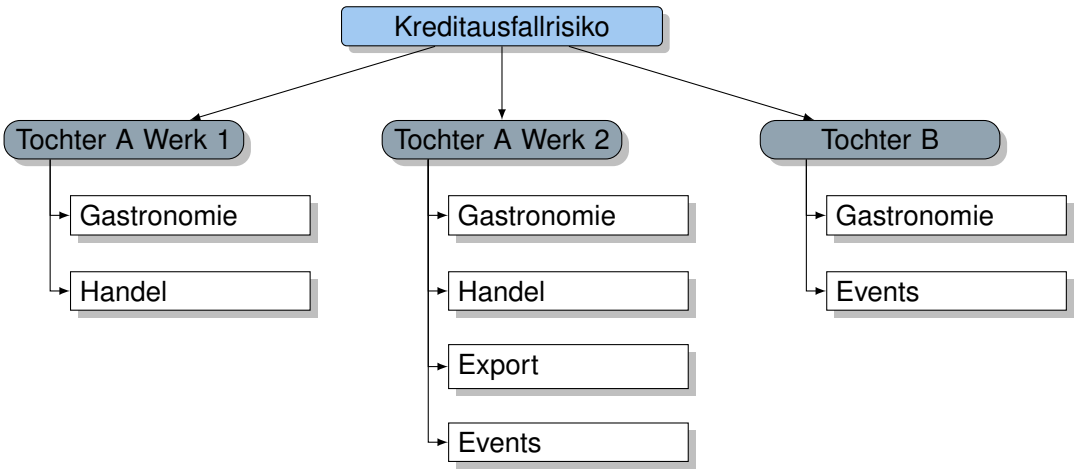


Abbildung 4.14: Beispielhafte Verteilung eines einzelnen Risikos über mehrere Bereiche des Unternehmens

Ereignis Nr.	Standort Nr.	Betrieb Nr.	Abt. Nr.	Indiv. Ereignis ID	Ereignis Name	Betrieb	Standort	Abteilung
2525	39	39	010	25253939010	Arbeitssicherheit	Tochter1	W1	Sondergeschäft
2600	38	38	901	26003838901	Unbefugter Zutritt	Tochter2	W3	Leitung
8500	00	20	701	85000020701	Default Risiko	Tochter3		Verkauf Handel
2350	00	11	931	23500011931	Counterparty Risiko	Holding		Treasury
2301	00	40	630	23010040630	Abhängigkeit von Konzernpartner	Tochter5		Logistik
4000	00	34	902	40000034902	Kartellrecht	Tochter4		Compliance
2075	00	11	920	20750011920	Datensicherheit und -schutz	Holding		IT
8010	00	20	701	80100020701	Stagnierender Markt	Tochter3		Verkauf Handel
8005	00	20	800	80050020800	Imageverlust	Tochter3		Marketing

Tabelle 4.5: Beispielhafte Einteilung der Risiken in einen Risikokonten Plan

Die Nummerierungslogik von Betrieb-, Standort- und Abteilungsnummer in Tabelle 4.5 wird hier nicht näher aufgelistet, sie ist ident dem Kontenplan der Finanzbuchhaltung entnommen. Die fünf Ereigniskategorien, als neutrale Formulierung der Risikokategorien in Tabelle 4.6, sind jeweils mit 2000 Nummern ausgestattet und sind ident mit jenen der Abbildung 4.8. Diese fünf Kategorien sind detailliert in Tabelle 4.6 aufgelistet und lauten Geschäfts- und strategische Risiken (engl. business-and-strategic-risk), betriebliche / operative Risiken (engl. operational-risk), compliance Risiken, Berichterstattung / Dokumentations Risiken (engl. reporting-risk) und wirtschaftliche Risiken (engl. commercial-risk). Leerstellen in der Nummerierung sind bewusst frei gelassen worden, um künftige Änderungen und Erweiterungen ohne eine Veränderung der bisherigen verwendeten Nummern zu ermöglichen.

0	**1999**	**Geschäfts- und strategische Risiken**
0	249	Marktbedingungen u. Technologie
0	24	Konsumverhalten
25	49	Projektentscheidungen
50	74	M&A
75	99	Geschäftsstrategie
100	124	Wetter

250	499	geistiges Eigentum und Reputation
250	274	Marken
275	299	Rezepte
300	324	Innovationen
500	749	Änderungen Rahmenbedingungen
500	524	Alkohol
525	549	Umweltauflagen
550	574	politische Veränderungen
575	599	Änderung rechtlicher Rahmenbedingungen
750	999	Singuläre Ereignisse
750	774	Höhere Gewalt
775	799	Sabotage
800	824	Naturereignisse
1000	1999	leer für künftige Änderungen

2000	**3999**	**Betriebliche/Operative Risiken**
2000	2249	Vermögens- und Infrastrukturrisiken
2000	2024	Gebäude
2025	2049	Maschinen und Betriebsmittel
2050	2074	Inventar, Vorräte und Wasserquelle
2075	2099	IT-Systemarchitektur und Datenschutz
2100	2124	Human asset
2250	2499	Projekt- und Tätigkeitsrisiken
2250	2274	Projektmanagement
2275	2299	Prozessmanagement
2300	2324	Group Relationship
2325	2349	Customer Management
2350	2374	Supplier Management
2375	2399	Counterparty Risiko
2400	2424	Organisation
2425	2449	Management quality & Business Continuity
2500	2749	Sicherheit und Umwelt
2500	2524	Arbeitszeiten
2525	2549	Personensicherheit
2550	2574	Umweltverschmutzung und -management
2575	2599	Lebensmittelsicherheit
2600	2624	Standortsicherheit
2750	3999	leer für künftige Änderungen

4000	**5999**	**Compliance Risiken**
4000	4249	Missachtung rechtlicher Bestimmungen

4000	4024	Missachtung von Gesetzen
4025	4049	Verordnung
4050	4074	Bewilligungen
4075	4099	Bescheide
4250	4499	Missachtung interner Vorgaben
4250	4274	Arbeitsanweisungen
4275	4299	Betriebsvereinbarungen
4300	4324	Richtlinien
4500	4749	strafrechtlich relevante Verstöße
4500	4524	kriminelle Energie von Dritten
4525	4549	kriminelle Energie durch Mitarbeiter
4750	5999	leer für künftige Änderungen

6000	**7999**	**Berichterstattungs/Dokumentations Risiken**
6000	6249	externe Berichterstattung
6000	6024	Börsenrecht
6025	6049	CGK
6050	6074	Veröffentlichung
6075	6099	Investor Relations
6250	6499	interne Berichterstattung, Kommunikation
6250	6274	Reports
6275	6299	Datenintegrität
6300	6324	Stammdaten
6500	6749	Wissens-, und Dokumentationsmanagement
6500	6524	Wissensmanagement
6525	6549	Dokumentationsmanagement
6750	7999	leer für künftige Änderungen

8000	**9999**	**Wirtschaftliche Risiken**
8000	8249	Marktrisiken
8000	8024	Absatzmarkt
8025	8049	Beschaffungsmarkt
8050	8074	Verkehrswertrisiken
8250	8999	Kreditrisiken
8500	8599	Ausfallsrisiken
8600	8699	Bürgschaftsrisiken
9000	9500	Finanzrisiken
9000	9099	Liquiditätsrisiken
9100	9199	Zinsänderungsrisiken
9200	9299	Währungsrisiken
9300	9399	Steuerrisiken

9400	9410	Bargeldlogistik
9500	9999	leer für künftige Änderungen

Tabelle 4.6: Beispielhafte Einteilung der Risiken und Risikokategorien mit Kontonummern nach Christoph Aichinger und Johann Grameder

Risikosteuerung und Kontrolle mittels Kennzahlen- und IT-unterstützter Früherkennung

Die Steuerung im Unternehmen soll mittelfristig anhand eines Frühwarnsystems aufgebaut werden, siehe Tabelle 4.8. Zusätzlich dient das Frühwarnsystem im Konzern auch als vorzügliche Kontrolleinrichtung.

Das Frühwarnsystem sollte nicht zu kompliziert aufgebaut sein, denn die Einfachheit erleichtert die Übersicht über die Zusammenhänge und die Kommunikation im Unternehmen. Die Indikatoren mit Frühwarneigenschaften müssen durch Kennzahlen messbar gemacht werden. Zahlen aus der Buchhaltung eignen sich als Früherkennungssignale nur bedingt, da sie im Allgemeinen erst spät und manchmal auch zu spät verfügbar sind. Dennoch gehören sie ebenso in ein umfassendes Früherkennungssystem, sind jedoch durch weitere Informationsquellen zu ergänzen. Weitere Details siehe Abschnitt 3.8.

Reporting, Überwachung und kontinuierliche Verbesserung

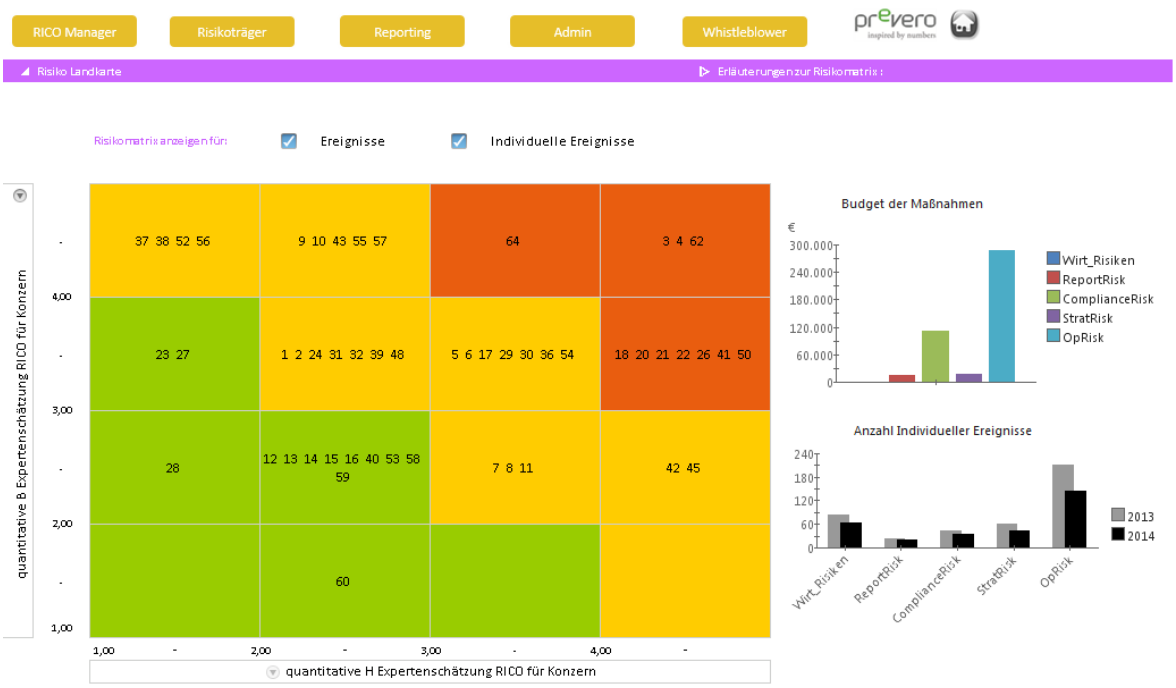
Die Sicherstellung der **Information und Kommunikation** ist die Hauptaufgabe des Risikomanagers, diese beinhaltet das Reporting, die Gestaltung von Dashboards (Ansichten von Einzelseiten im Informationssystem) und die periodischen Abhaltungen von Schulungen und Risikomanagement Sitzungen.

- Ein periodisch wiederholter Risikoprozess ist notwendig, da sowohl Bedeutung, Häufigkeit als auch Zusammenhänge von Risiken einer zeitlichen Veränderung unterliegen.
- Der Fortschritt in der Risikobewältigung gehört anhand des Maßnahmenplans überwacht und per Projekt- und Performancemanagement gemessen.
- Ein Frühwarnsystem mit schwachen Signalen und regelmäßiger Pflege von KPIs (key-performance-indicator) wird im Zuge der Überwachung empfohlen. Ebenso die detaillierte Untersuchung bereits eingetretener Ereignisse.

In Abbildung 4.15 wird für die Kontrolle eine ähnlich Portfolioansicht mittels Risikomatrix eingesetzt, wie in der Beurteilung nach Abbildung 4.9 und Steuerung nach Abbildung 4.10. Die abgerufenen und angezeigten Werte und Dimensionen können beliebig, je nach Methode und Geschmack der Kontrolleure angepasst werden.

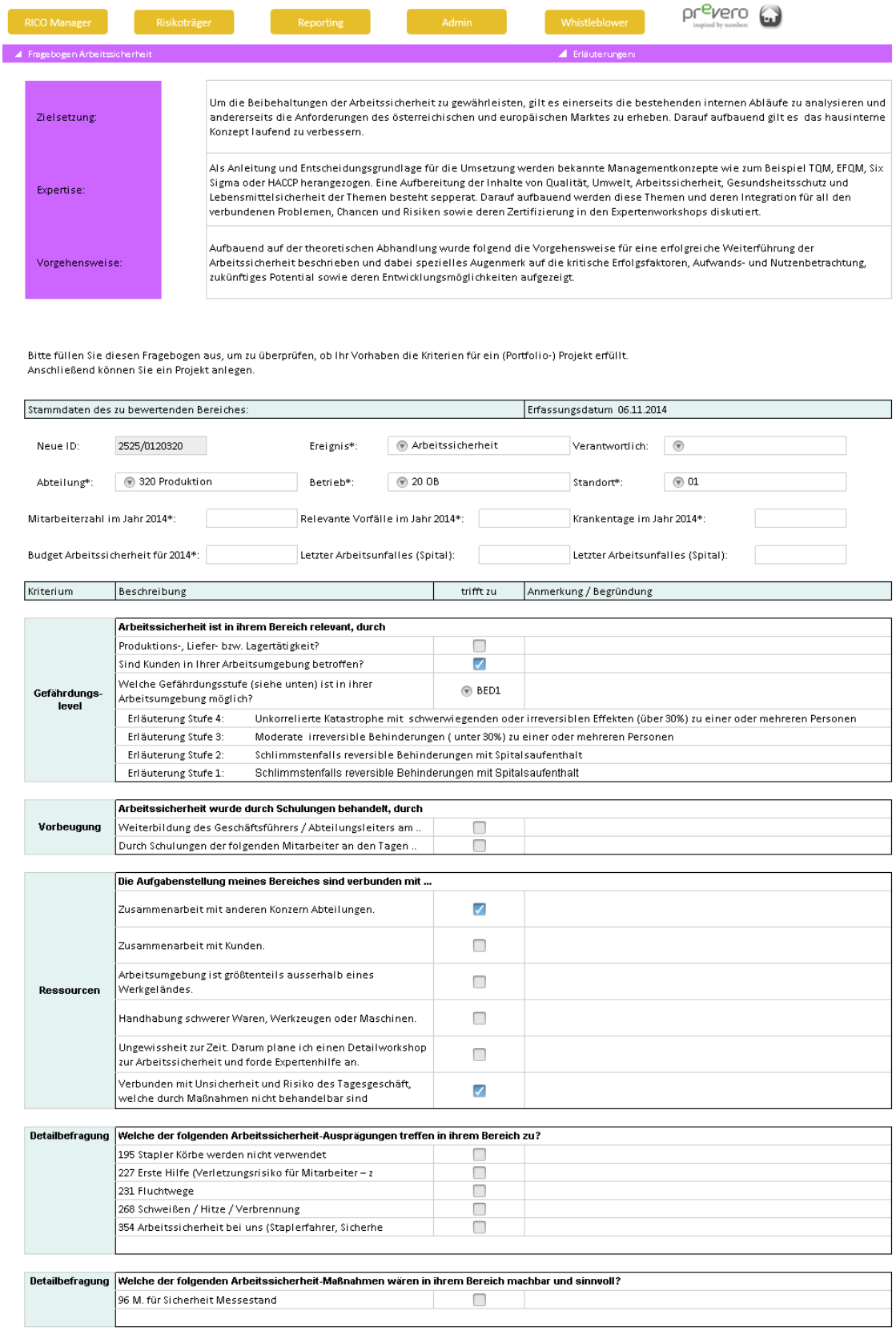
Beobachtungsbereiche	Indikatoren mit guten Frühwarneigenschaften
Konjunkturelle Entwicklung	- Auftragsentwicklung der Branche
	- amtliche Auftragseingänge
	- kommende Gesetzesänderungen
Technologische Entwicklung	- Informationen über mögliche Änderungen der Verfahrenstechnologie
	- Informationen über mögliche Änderungen der Produkttechnologie
Produkte und Regionen des Absatzmarktes	- eigene Auftragseingänge
	- eigene Auftragsbestände
	- Länderübersicht und -risiken
Kunden der Unternehmens	- Bestell- und Einkaufsverhalten
	- Nachfragevolumen wichtiger Kunden
	- Forderungsumschlagzeit
	- Zahlungsziele
	- Auftragseingänge bei wichtigen Kunden
Konkurrenten der Unternehmung	- Preispolitik
	- Programmpolitik
Lieferanten der Unternehmung	- Preise und Konditionen der Lieferanten
	- Beschaffungspreise im Vergleich zur Konkurrenz
Kapitalmarkt	- Zinsen
	- Wechselkurse
Produktionsprogramm	- Anteil von erfolgreichen und problematischen Produkten
	- Anteil der Produkte im Portfolio
Mitarbeiter	- Lohn- und Gehaltszuwächse
	- Fehlzeiten
	- Fluktuationen
Ergebnis- und Finanzlage	- Rentabilität (Hochrechnung)
	- Betriebs- und Unternehmensergebnis (Hochrechnung)
	- Cashflow (Hochrechnung)
	- Liquiditätsreserve (Hochrechnung)
Forschung und Entwicklung	- Entwicklungszeiten im Vergleich zur Konkurrenz
	- F & E-Kosten im Vergleich zur Konkurrenz
Absatz	- Umsatzerlöse (Hochrechnung)
	- Marktanteile
	- Preise (Netto)
	- Lagerbestände im Vergleich zur Konkurrenz
	- Umschlaghäufigkeit der Waren
Produktion und Beschaffung	- Durchlaufzeit
	- Ausstoß (Hochrechnung)
	- Ausschuss
	- Lohnkosten (Hochrechnung)
	- Lohnkostenanteil im Vergleich zur Konkurrenz
	- Beschaffungspreise und Konditionen im Vergleich zur Konkurrenz
	- Geräteauslastung

Tabelle 4.8: Gängige Frühindikatoren im Risikomanagement



ID	Ereignis	Status	Geändert	Verantw. Experte	Budget	BED.	HÄU.	VaR.	AP-Zahl:	M-Zahl:	TOP
											all
1	8050 Verkehrswertänderung	aktiv	16.5.14			3	2		3		
2	8025 Einkaufspreisänderung	aktiv	16.5.14		€ 0	3	2	€ 16.000	5	1	
3	8020 Marktveränderung	aktiv	17.5.14		€ 3.000	4	4	€ 18.999	11	2	
4	8011 Kundenkonzentration	aktiv	16.5.14			4	4	€ 3.000	4		☑
5	8010 Stagnierender Markt	aktiv	16.5.14		€ 0	3	3	€ 26.000	4	1	☑
6	8000 Sinkende Wirtschaftlichkeit der Besta	aktiv	16.5.14			3	3	€ 16.000	2		
7	8500 Default Risiko	aktiv	17.5.14		€ 0	2	3	€ 49.999	38	1	
8	8522 Prüfung der Wirtschaftlichkeit nachträg	aktiv	16.5.14			2	3	€ 12.000	7		
9	8275 Bürgschaftsrisiko	aktiv	16.5.14			4	2	€ 1.000			
10	8252 Prüfung der Wirtschaftlichkeit vorab fel	aktiv	17.5.14		€ 5.000	4	2	€ 20.999	4	2	
11	8251 Kundenschönrechnung	aktiv	16.5.14			2	3	€ 21.000	7		☑
12	9000 Liquiditätsrikio	aktiv	16.5.14			2	2	€ 5.000	2		
13	9020 Gebundene Kapital im Umlaufvermöge	aktiv	16.5.14			2	2	€ 10.000			
14	9100 Zinsänderungsrisiko	aktiv	16.5.14			2	2	€ 1.000	1		
15	9200 Wechselkursrisiko	aktiv	16.5.14			2	2	€ 5.000	2		
16	9300 Steuerrisiko	aktiv	16.5.14			2	2		2		
17	6300 mangelnde Stammdaten	aktiv	17.5.14			3	3	€ 13.000	6		
18	6275 mangelnde Datenintegrität	aktiv	16.5.14			3	4	€ 26.999	7		
19	6075 Investor Relations	aktiv									
20	6500 Wissensmanagement	aktiv	16.5.14		€ 16.000	3	4	€ 5.000	4	6	
21	6525 mangelnde Dokumentation von Änder	aktiv	16.5.14			3	4	€ 3.000	1		
22	6526 Dokumentationspflichten	aktiv	16.5.14			3	4	€ 10.999	8		
23	4010 Sonstige Gesetzeskonformität	aktiv	16.5.14		€ 15.000	3	1	€ 16.000	16	2	
24	4000 Kartellrecht	aktiv	17.5.14		€ 3.000	3	2	€ 20.999	6	1	☑
25	4250 Missachtung von Vorschriften durch Mi	aktiv	17.5.14		€ 69.000			€ 26.000	32	25	
26	4275 mangelhaftes Berechtigungskonzept	aktiv	24.9.14		€ 3.000	3	4	€ 21.999	10	2	
27	4300 Mangelnde Kontrollen (4 Augen Prinzip	aktiv	16.5.14		€ 22.000	3	1	€ 26.000	12	4	
28	4500 kriminelle Energie von Außen	aktiv	16.5.14		€ 0	2	1	€ 11.000	14	1	
29	0100 Wetter Risiko	aktiv	16.5.14	Administrator		3	3	€ 8.000	1		

Abbildung 4.15: Prototypische Umsetzung der Kontrollansicht mit Portfolioblick auf Risiken und Maßnahmen



RICO Manager | Risikoträger | Reporting | Admin | Whistleblower | prevero

Fragebogen Arbeitssicherheit — Erläuterungen:

Zielsetzung:	Um die Beibehaltungen der Arbeitssicherheit zu gewährleisten, gilt es einerseits die bestehenden internen Abläufe zu analysieren und andererseits die Anforderungen des österreichischen und europäischen Marktes zu erheben. Darauf aufbauend gilt es das hausinterne Konzept laufend zu verbessern.
Expertise:	Als Anleitung und Entscheidungsgrundlage für die Umsetzung werden bekannte Managementkonzepte wie zum Beispiel TQM, EFQM, Six Sigma oder HACCP herangezogen. Eine Aufbereitung der Inhalte von Qualität, Umwelt, Arbeitssicherheit, Gesundsheitsschutz und Lebensmittelsicherheit der Themen besteht sepperat. Darauf aufbauend werden diese Themen und deren Integration für all den verbundenen Problemen, Chancen und Risiken sowie deren Zertifizierung in den Expertenworkshops diskutiert.
Vorgehensweise:	Aufbauend auf der theoretischen Abhandlung wurde folgend die Vorgehensweise für eine erfolgreiche Weiterführung der Arbeitssicherheit beschrieben und dabei spezielles Augenmerk auf die kritische Erfolgsfaktoren, Aufwands- und Nutzenbetrachtung, zukünftiges Potential sowie deren Entwicklungsmöglichkeiten aufgezeigt.

Bitte füllen Sie diesen Fragebogen aus, um zu überprüfen, ob Ihr Vorhaben die Kriterien für ein (Portfolio-) Projekt erfüllt.
Anschließend können Sie ein Projekt anlegen.

Stammdaten des zu bewertenden Bereiches:					Erfassungsdatum 06.11.2014
Neue ID:	2525/0120320	Ereignis*:	Arbeitssicherheit	Verantwortlich:	
Abteilung*:	320 Produktion	Betrieb*:	20 OB	Standort*:	01
Mitarbeiterzahl im Jahr 2014*:		Relevante Vorfälle im Jahr 2014*:		Krankentage im Jahr 2014*:	
Budget Arbeitssicherheit für 2014*:		Letzter Arbeitsunfalles (Spital):		Letzter Arbeitsunfalles (Spital):	

Kriterium	Beschreibung	trifft zu	Anmerkung / Begründung
Gefährdungs-level	**Arbeitssicherheit ist in ihrem Bereich relevant, durch**		
	Produktions-, Liefer- bzw. Lagertätigkeit?	☐	
	Sind Kunden in Ihrer Arbeitsumgebung betroffen?	☑	
	Welche Gefährdungsstufe (siehe unten) ist in ihrer Arbeitsumgebung möglich?	BED1	
	Erläuterung Stufe 4:	Unkorrelierte Katastrophe mit schwerwiegenden oder irreversiblen Effekten (über 30%) zu einer oder mehreren Personen	
	Erläuterung Stufe 3:	Moderate irreversible Behinderungen (unter 30%) zu einer oder mehreren Personen	
	Erläuterung Stufe 2:	Schlimmstenfalls reversible Behinderungen mit Spitalsaufenthalt	
	Erläuterung Stufe 1:	Schlimmstenfalls reversible Behinderungen mit Spitalsaufenthalt	
Vorbeugung	**Arbeitssicherheit wurde durch Schulungen behandelt, durch**		
	Weiterbildung des Geschäftsführers / Abteilungsleiters am ..	☐	
	Durch Schulungen der folgenden Mitarbeiter an den Tagen ..	☐	
Ressourcen	**Die Aufgabenstellung meines Bereiches sind verbunden mit ...**		
	Zusammenarbeit mit anderen Konzern Abteilungen.	☑	
	Zusammenarbeit mit Kunden.	☐	
	Arbeitsumgebung ist größtenteils ausserhalb eines Werkgeländes.	☐	
	Handhabung schwerer Waren, Werkzeugen oder Maschinen.	☐	
	Ungewissheit zur Zeit. Darum plane ich einen Detailworkshop zur Arbeitssicherheit und forde Expertenhilfe an.	☐	
	Verbunden mit Unsicherheit und Risiko des Tagesgeschäft, welche durch Maßnahmen nicht behandelbar sind	☑	
Detailbefragung	**Welche der folgenden Arbeitssicherheit-Ausprägungen treffen in ihrem Bereich zu?**		
	195 Stapler Körbe werden nicht verwendet	☐	
	227 Erste Hilfe (Verletzungsrisiko für Mitarbeiter – z	☐	
	231 Fluchtwege	☐	
	268 Schweißen / Hitze / Verbrennung	☐	
	354 Arbeitssicherheit bei uns (Staplerfahrer, Sicherhe	☐	
Detailbefragung	**Welche der folgenden Arbeitssicherheit-Maßnahmen wären in ihrem Bereich machbar und sinnvoll?**		
	96 M. für Sicherheit Messestand	☐	

Abbildung 4.16: Prototypische Umsetzung der Kontrolle von Risiken durch online Befragung

Abbildung 4.16 zeigt eine periodische Befragung der Risikosituation mittels Fragebogen. Dabei sind die Eingaben der Vorperiode grauschattiert eingeblendet und können bei unveränderter Lage belassen oder bei Veränderungen neu eingegeben werden. Diese Fragebogenmethode ist vor allem bei gutbeherrschten und eher ungefährlichen Risikopotentialen eine effiziente Methode, wobei Neubewertungen in Form von Expertenworkshops auch hier in längeren Abständen zu empfehlen sind.

Die vorhandenen Fragebögen können auch in abgewandelter Form als Prüfbögen bei Audits oder Kontrollen zum Einsatz kommen.

4.6 Kapitel 4 - IT Konzeption des Risikomanagementsystems

Dieses Kapitel dient der Übersicht und Weiterleitung auf die passenden Quellen und Dokumente bezüglich dem Informationssystem.

Eine Übersicht über das verwendete Informationssystem, Zugangsmöglichkeit, Administratorkontakte und der wichtigsten Grundlagen kann als Kapitel, Anhang oder eigenes Risikomanagement-IT-Handbuch umgesetzt werden. Details und ein Vorschlag für dieses hier leer gelassene Handbuch Kapitel findet man im Kapitel 6.

4.7 Kapitel 5 -Geltungsbereich, Inkrafttretung, Versionierung, Anhänge

Geltungsbereich des Risikomanagementhandbuch

Das in der aktuellen Version gültige Risikomanagement-Handbuch ist für die am Titelblatt angeführten Gesellschaften und deren Mitarbeiter gültig. Die Verantwortlichen im Risikomanagement sind ebenfalls auf der Titelseite angeführt. Die jeweilige Geschäftsführung setzt das Risikomanagement-Handbuch mittels Beschluss in Kraft. Das Risikomanagement-Handbuch wird allen Mitarbeitern im Intranet zur Verfügung gestellt und ist somit für jeden Mitarbeiter immer einsehbar. Die Versionierung mit Änderungsliste ist im ist im Abschnitt 4.7 ersichtlich. Die auch nur teilweise Weitergabe des Risikomanagement-Handbuchs an dritte, nicht unternehmenszugehörige Personen ist vorab mit der Risikomanagement Leitung abzuklären!

Inkrafttretung des Risikomanagementhandbuch

Die Geschäftsführung setzt das Risikomanagementhandbuch mittels Beschluss in Kraft.

Das Risikomanagementhandbuch wird den Mitarbeitern im Intranet zur Verfügung gestellt.

Versionierung und Auflistung der Anhänge des Risikomanagementhandbuch

Die Versionierung hat vollständig und ausschließlich dokumentiert mit der Änderungsliste in Tabelle 4.9 vollzogen zu werden. Sie dient in weiterer Folge als Dokumentenhistorie und ist auch rechtlich relevant!

Version	ÜberarbeiterIn	Datum	Freigabe	Beschreibung der Änderung
1.0	Martin Marenich	18.12.2014	Vorstand	Einführung

Tabelle 4.9: Beispielhafte Versionierung und Auflistung des Risikomanagementhandbuchs und dazugehöriger Anhänge

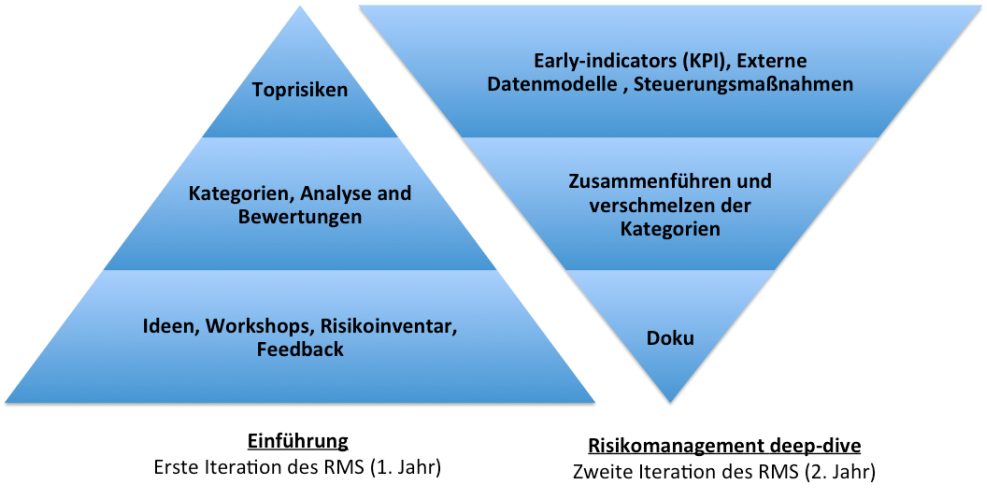


Abbildung 4.17: Der Einführungsprozess - Es gibt kein richtig oder besser - RMS ist ein iterativer Prozess

4.8 Erfahrungsbericht aus dem Risikomanagementsystem Einführungsprozess

Dieses Kapitel beschäftigt sich mit den gemachten Erfahrungen, im Zuge der Recherchen, Gesprächen und dem vollzogenen Einführungsprojekt mit beiden Kooperationspartnern. Prinzipiell folgte das gesamte Forschungsprojekt dem fast zweijährigem Ablauf nach Abbildung 4.17.

Die folgende Auflistung zeigt in komprimierter Form Ideen, Probleme, Erfahrungen und Ergebnisse und gliedert diese anhand der bereits im vorigen Kapitel verwendeten Struktur.

- **Ermittlung des internen Umfelds:**

Ergebnis Die prinzipielle Herangehensweise muss zu beginn der Einführung getroffen werden, ob der Risikomanagementprozess top-down oder bottom-up erfolgen soll, siehe Ab-

schnitt 3.9. Die gewählte Methode muss mit dem tone-of-the-top der Unternehmensführung zusammenpassen.

Ergebnis Ein Kickoff für das Risikomanagement 2.0 Einführungsprojekt wurde mit dem Vorstand abgehalten, das Vorgehen abgesprochen und Unterstützung eingeholt. Wie in Abschnitt 3.3 erläutert ist die starke Unterstützung der Unternehmensführung unerlässlich.

Ergebnis Regelmäßige Berichte an die Geschäftsführung über die Entwicklung des Risikomanagements sollten in Besprechungen oder per Newsletter erfolgen.

Idee Die Risikokultur, als kritische Erfolgskomponente, bedarf eine Einbindung aller Mitarbeiter und damit einen Fokus auf Schulung, Training und Beobachtung der vorherrschenden Praxis. Dazu gehört dass Transparenz, freier Informationsfluss und Gesprächskultur gefördert werden. Risikobewusstsein und Risikoverantwortung sollten im ganzen Unternehmen verbreitet werden. Ob dieser Ansatz erfolgsversprechender ist als die pure Risikoquantifizierung oder beide gleich bedeutend für ein erfolgreiches Risikomanagement sind, bleibt abzuwarten.

Idee Gerade im Risikomanagement mit den vielen Prozessschritten sollte man von anderen lernen! Auch die Nutzung einer evolutionären Einführung mit kontinuierlicher Verbesserung erscheint sinnvoll. Der Weg ist das Ziel!

Ergebnis Risikomanagement behandelt und betrifft vor allem Menschen!

Problem Die Wirtschaftlichkeit muss permanent überblickt werden, da im Risikomanagement stets viele Mitarbeiter involviert sind, die viele unterschiedliche Ideen, Methoden und Gewohnheiten haben.

Ergebnis Risikomanagement ist Vermeidung von Risiken und Mitnahme von Chancen!

- **Identifikation:**

Ergebnis Im ersten Identifikationsdurchgang der Partnerfirma mittels Expertenworkshops wurden an 12 halbtägigen Workshops mit 67 Teilnehmern insgesamt 880 Risiken erhoben. Diese 880 Risiken bilden das Risikoinventar der Firma. Zusätzlich konnten am Ende der jeweiligen Workshops bereits insgesamt 66 Risikokategorien gebildet werden, die später größtenteils als Toprisiken übernommen und qualitativ mittels Scoring bewertet wurden. Die Expertenworkshops waren in Finanzbuchhaltung und Treasury, Controlling, EDV, Eventmanagement und PR, Lager und Logistik, Produktion und Qualität, Personalwesen, Verkauf Gastronomie, Verkauf Handel und Marketing, Einkauf, Konzerntochter 1 und Konzerntochter 2 aufgeteilt. Jeder Workshop generierte bereits Maßnahmen und Verbesserungsvorschläge, die auf jeden Fall dokumentiert gehören! Dieses Beispiel zeigt, dass die Identifikation gedanklich einer Siebmaschine gleicht, man braucht mehrere und immer feinere Filter!

$Erfahrung$ Bei den Expertenworkshops braucht es grundsätzlich einen pragmatischen und lösungsorientierten Zugang aller Beteiligten. Die TeilnehmerInnen müssen zu beginn persönlich eingebunden werden, durch eine methodische Einführung, z.B. ice-breaker-games oder Vorstellungsrunden. Die Meinung der Teilnehmer ist ernst zu nehmen, ebenso die Umgangsformen und Feedbackregeln. Die Moderation ist daher ein kritischer Erfolgsfaktor, da sie den Spagat zwischen oberflächlicher und detailverliebter Risikodiskussion, vielredenden und schüchternen TeilnehmerInnen und fachspezifischen und unternehmensweiten Prozessen bewältigen muss. Letzten Endes sollen die Ergebnisse einheitlich aufgearbeitet sein, trotz verschiedener Gruppenzusammensetzungen, Schwerpunktthemen und Traditionen.

$Erfahrung$ Eine umfangreiche Dokumentation der Diskussionspunkte, etwaige Lösungsvorschläge, Meinungsverschiedenheiten im Diskurs, vergangenen Maßnahmen, Ideen, Zusammenhänge etc. ist notwendig. Oft werden Begriffe aus der Praxis verwendet, welche durchaus in Form von Ausprägungen in das offizielle Risikomanagementsystem eingepflegt werden können.

$Idee$ Verpflichtendes Vorarbeiten für die TeilnehmerInnen des Workshops in Form von Daten, Unterlagen, Berichten oder Risikofragebögen können zumindest bei bekannten Risiken eine fundiertere Diskussion und Einschätzung bringen. Eventuell sprengt es aber gerade bei der ersten Workshoprunde den Rahmen.

$Problem$ In der zweiten Hälfte des halbtägigen Workshops wurden die in der ersten Hälfte gefundenen und besprochenen Risiken in Kategorien geclustert. Anschließend wurden sie mittels der Scoringmethode mit Punkten erstmalig qualitativ bezüglich Bedeutung und Häufigkeit beurteilt. Dabei hatte jede Gruppe nur ihre eigenen Risikokategorien zu beurteilen. Festzuhalten ist, dass gerade diese Erhebungsmethodik zwar ein strukturiertes Vorgehen ermöglichte aber zu folgenden Problemen führte:

* Keinen unternehmensweiten Rahmen um Risiken verschiedener Abteilungen und Kategorien miteinander objektiv zu vergleichen und zu reihen. Beispielsweise waren 18 Scoring Bedeutungspunkte im Einkauf nicht mit 18 Punkten im Verkauf vergleichbar, da unterschiedlich viele Personen in jeder Workshopgruppe teilnahmen und eine unterschiedliche Anzahl an Kategorien bewertet wurde.
* Die Objektivität der Ergebnisse muss nachträglich durch Experten kritisch überprüft werden, denn Gruppenteilnehmer können strategisch wählen, die Bewertung missverstanden, einzelne offensichtliche Toprisiken über versteckte Toprisiken dominiert haben oder fehlende quantitative Daten den wahren Umfang täuschen.
* Missverständnisse sind im Verständnis zwischen Bedeutung (als Konsequenz durch durchschnittliche Verlustmöglichkeit) und Häufigkeit (des Auftretens bzw. Wahrscheinlichkeit) aufgetreten. So muss klar hingewiesen werden, dass bei der Bedeutung, die des einzelnen Ereignisses gemeint ist und

Abteilung	Inkl. Bewertung	Ereignisse, Risiken und Chancen	Ideen und Maßnahmen	Mitglieder
Finanzbuchhaltung & Treasury	☑	57	undokumentiert	8
Controlling	☑	64	39+	8
EDV	☑	47	7+	6
Eventmanagement und PR	☑	24	36	4
Lager und Logistik	☑	33	31+	5
Produktion und Qualität	☑	23+	14	7
Personalwesen	☑	57	6	4
Verkauf Gastronomie	☑	61	33+	6
Verkauf Handel und Marketing	☑	48	12	6
Einkauf	☑	28	22	6
Konzerntochter 1	☑	31	37	1

Abbildung 4.18: Expertengespräche zur Risikoidentifikation und Bewertung als facilitated-workshops

nicht die Gesamtbedeutung dieses Risikos (durch etwa häufige aber niedrige Risiken).

Erfahrung Eine wichtige Herausforderung beim erfassen und analysieren von Daten, ist es keine unnütze Datenflut zu produzieren. Seitenweise Protokolle ersetzen keine gutgegliederte Tabelle. Die sinnvolle Reduktion der Komplexität und passende Verdichtung macht Risikodaten erst handhabbar, ein wichtiger Erfolgsfaktor!

- **Beurteilung:**

Ergebnis Im nächsten Schritt wurde das Risikoinventar analysiert. Die 66 Toprisiken hatten ca. 300 Risiken aus dem Brainstorming zugeordnet, welche Ausprägungen genannt wurden. Die Ausprägungen stellen somit als unternehmensbezogene Beispiele einen Realitätsbezug zu dem oft generischen Wortlaut einer Toprisikobenennung. Beispielsweise wurde dem Toprisiko Arbeitssicherheit mit Ausprägungen wie Staplerverkehr, Gebäudezustand, Außendienst oder Arbeitshandbuch eine konkrete Situationsbeschreibung gegeben. Die 66 Toprisiken wurden dem Vorstand mittels Risikomatrix zwischendurch präsentiert, inklusive dem Entwurf eines Risikostammblattes für künftige Systemimplementierung.

Idee Für 39 Topisiken wurde eine Detailanalyse durchdacht, um ein besseres Verständnis aufzubauen. Weitere Detailanalysen wurden für die nächste Projektphase vorgeschlagen.

$Ergebnis$ Das zentrale Risikomanagement Team tagte ein halbes Jahr nach der Identifikation rund 20 mal und im Schnitt 2,5 Stunden. Die vier TeilnehmerInnen setzten sich aus Risikomanagement, IKS und Compliance zusammen.

$Problem$ Bei der Zuordnung der 880 Risiken in den Risikokategorien nach Abschnitt 4.5 wurden im ersten Schritt mehrfache Zuordnungen zugelassen. Durchschnittlich konnte jedes Risiko in 1,64 Kategorien zugeteilt werden, insgesamt betraf das 484 Risiken mit 2 Kategorien und 42 mit 3 Kategorien. Die dabei entstandene Genauigkeit und Interdependenzen wurden aufgrund des hohen Aufwandes von 6 vollzeitäquivalenten Tagen nicht weiter verfolgt. Die Interdependenzen hätten eine Korrelationsmatrix bedürft und somit eine prozentuelle Aufteilung jedes Risikos nach Kategorien. Die Berechnung von Korrelationen braucht eine umfangreiche Datenanalyse, diese Daten müssen im Unternehmen vorhanden sein.

$Problem$ Die Frage ob man Risikokategorien braucht wird hier beleuchtet:

- $+$ Hilft bei vielen Risiken die Übersicht zu bewahren
- $+$ Durch die Kategorien können Aufgabenbereiche verteilt und Expertenkreise gebildet werden.
- $+$ Im IT System können Verknüpfungen zwischen Kategorien und anderen Dimensionen wie Methoden, Ausprägungen, Unternehmensbereichen, Skalen, Daten, u.v.m. die Anzahl der Verknüpfungen und Unübersichtlichkeit dramatisch verringern!
- $+$ Kategorien fördern Verständnis und Übersicht beim Management, Mitarbeitern und allen weiteren Stakeholdern.
- $+$ Die Kategorien, mit Auflistung ihrer Toprisiken, dienen als übersichtliche Checkliste. Da sie an alle MitarbeiterInnen kommuniziert werden kann, fallen fehlende Toprisiken leichter auf!
- $-$ Aufgrund der relativ wenigen Risikokategorien sind die darin zusammengefassten Einzelrisiken recht inhomogen und für unerfahrene Leser nicht intuitiv zusammenhängend.
- $-$ Die teilweise Inhomogenität innerhalb der Risikokategorien sind ein Problem für Interdependenzen, Aggregierungen oder Datenbankverknüpfungen.
- $-$ Mit der Zeit werden die einzelnen Risikokategorien relativ groß, da viele Versionierungen, Varianten, Ausprägungen und viele weitere Daten daran hängen. Ob dies mit einer langfristigen feineren Aufteilung oder periodischen Entrümpelungen zu lösen ist bleibt offen.
- o Beide Methoden, die der vorgefertigten bzw. standardisierten Risikoklassen vor dem Workshop oder eine gemeinsame Erarbeitung, etwa durch clustering während des Workshops, haben Vor- und Nachteile!

$Erfahrung$ Nicht alle theoretisch möglichen Toprisiken sind wesentlich, da sie entweder über keine Priorität verfügen oder so unwahrscheinlich sind, dass nicht einmal ein Krisenplan sinnvoll erscheint. Andere Toprisiken können so heikel sein, dass deren Dokumentation Feingefühl bedarf und sofortige Maßnahmen zu ergreifen sind.

Für den Risikomanager gilt es einen kühlen Kopf zu bewahren und gegebenenfalls seine Funktion mittels Eskalation nach oben auszufüllen.

$Erfahrung$ Die Einsichtnahme in die Datenquellen kann mitunter schwer zugänglich sein oder es können sogar gar keine Datenquellen vorhanden sein. Aus den traditionell verschieden aufgebauten Unternehmensbereichen können eine Vielzahl bestehender Vorgaben, Kennzahlen, Datenbanken, Datenformate oder Einheiten nebeneinander existieren. Diese müssen bei Bedarf vereinheitlicht werden.

$Problem$ Eine Streitfrage bleibt die notwendige Bürokratie und Dokumentation eines Risikomanagement! Die Häufige Kritik ist, dass bei einer Überbürokratisierung die eigentliche Tätigkeit wie Risiken durch Früherkennung und schwache Signale zu verhindern vernachlässigt wird. Unter Überbürokratisierung können bereits unnötige Genauigkeit bei der Kategorisierung von Risiken, Behandlung zu vieler unwichtiger kleiner Risiken oder übervolle Risikostammblätter fallen. Puristen unter den Risikomanagern behaupten, es gehe generell um die wenigen wichtigen Toprisiken und nicht um die Unzahlen an Trivialen. Dies führt zum top-down Ansatz der Risikobeurteilung.

$Ergebnis$ Da zu einem Großteil der Risiken wenig analysierbare Daten vorlagen und deren Erhebung enorme Ressourcen bedurft hätte, erfolgten die Korrelationen nur mittels 1 für 100% und 0 für 0%. Dies entsprach einer eindeutigen Zuordnung und demnach wurden alle Mehrfachzuordnungen ersetzt und jedes Risiko nur der relevantesten und dominantesten Risikokategorie zugeordnet.

$Ergebnis$ Dabei diskutierte man erneut die Zuordnung aller Risiken in eine der Kategorien, die dann einfachheitshalber zu den Toprisiken avancierten. Es kristallisierten sich die rund 60 Toprisiken heraus, denen letztlich alle 880 ursprünglichen Risiken als Ausprägungen zugeteilt wurden. Jedem Toprisiko wurden die Maßnahmen, Detailerklärungen und Bewertungen aus den Workshops hinzugefügt. Sie wurden mit weiteren Merkmalen bewertet, beispielsweise ob diese zusätzliche Kontrollen erforderten, wesentliches Chancenpotential beinhalteten oder welche verantwortlichen Unternehmensbereiche diese tragen. Ebenfalls wurden Prioritäten zugeteilt, um die Kritischsten für den Vorstand zu sortieren.

$Ergebnis$ Da jedes Toprisiko mehrere Verantwortliche in einem Konzern hat, wurde jedem Verantwortlichen ein eigenes Stammblatt als s.g. individuelles Risiko bereitgestellt. Insgesamt wurden so über 300 Stammblätter für individuelle Risiken angelegt. Beispielsweise braucht das Toprisiko Arbeitssicherheit alleine 20 Stammblätter für individuelle Risiken, das Defaultrisiko 15 und das Liquiditätsrisiko, da nur das Treasury zuständig ist, nur ein Einziges. In einem Stammblatt für individuelle Risiken kann jeder Verantwortliche eine Zuteilung der zutreffenden Ausprägungen, Bewertungen und passenden Maßnahmen für seinen Unternehmensbereich auswählen. Diese zuerst als Microsoft Excel erstellten Arbeitsblätter wurden schließlich in die Software übertragen.

$Ergebnis$ Jedem Toprisiko wurde eine Bewertungsmethodik wie VaR oder Expertenschätzungen vorgeschrieben, um eine Aggregierung innerhalb der Risikokategorien

zu ermöglichen. Dem Gesamtunternehmen und jedem Unternehmensbereich wurden vierstufige Skaleneinträge für Bedeutung und Häufigkeit vorgeschlagen.

$Problem$ Risiken bei denen die Häufigkeit hoch und die Bedeutung (EUR) niedrig ist, müssen nicht zwangsläufig Toprisiken sein. Oftmals gibt es gerade für diese Risiken passende Methoden!

$Problem$ Bei Risiken bei denen sowohl Häufigkeit als auch Bedeutung hoch sind, muss die Beurteilung kritisch hinterfragt werden. Denn seitens der Logik sollte es diese Fälle in einem solventen Unternehmen nicht geben.

$Problem$ Die Verbindung von Zielsetzung und Risiko gestaltete sich schwierig. Alle Ziele abseits der finanziellen müssen in einem mittelständischen Unternehmen, ohne vorhandenen balance-score-card System, zusammengesucht, ausformuliert, abgeklärt und als zusätzliche Dimension in die Datenbankstruktur eingepflegt werden. Ob dies in kleineren Unternehmen nötig ist, bleibt fraglich!

$Problem$ Die folgende persönliche Einschätzung gilt bei unternehmensweiten Risikomanagement und somit außerhalb der einzelnen Methodenkompetenz in den Finanz- und Technikabteilungen. Bei den im Zuge dieser Arbeit rund einem dutzend befragten mittelständischen Nichtfinanzunternehmen haben die etablierten Methoden zur Risikoquantifizierung ein bescheidenes Ausmaß. Oft gehen sie über eine einfache Expertenschätzung nicht hinaus. Dies erfolgt dann meist in Form einer semiquantitativen Risikomatrix mit einer vier-, fünf oder sechsteiligen Skala für die beiden Dimensionen Häufigkeit und Bedeutung. Die Aggregierungen, Priorisierungen oder Korrelationen wurden, wenn überhaupt, durch eine erneute Expertenschätzung der gruppierten Einzelrisiken als Gruppenrisiko vollzogen.

$Problem$ Es herrscht bei vielen nicht finanziellen Risikokategorien Datenarmut. Somit ist die Grundlage von mathematisch-statistischen Methoden nicht gegeben, denn “junk data in means junk data out”. Am Rande sei erwähnt, dass auch Datenreichtum ein Problem darstellen kann. Denn bei sogenannten “data-rich” Modellen sind die Probleme verkehrt proportional zu jenen der “data-poor” Modelle und zu viele Daten führen zu keinen eindeutigen Ergebnissen.

$Problem$ Der externe Zukauf dieses Datenmaterials ist denkbar, eine Risikoberechnung auf Basis ausschließlich externer Daten wird nicht empfohlen. Externe Daten sollten als Kontrolle, Vergleich oder Erweiterung der internen Daten genutzt werden. Die Argumentation gegen ausschließlich externe Daten in Form von z.B. Branchendaten ist, dass auf den realen unvollkommenen Märkten unternehmensinterne Daten mehr Informationen über die Risikosituation des eigenen Unternehmens liefern können. Gerade dieser Kritikpunkt des vermissenden Bezugs zum Unternehmen ist jedoch beim Risikomanagement sehr relevant!

$Problem$ Vor geschätzten Korrelationen, nicht zutreffenden Verteilungsdichten oder schlecht recherchierten internen und externen Daten zur Quantifizierung kann nur gewarnt werden! Im Auge des Autors ist die Quantifizierung aller Risikokategorien und deren Aggregierungen für Mittelstandsbetriebe somit im Jahr 2014 noch

nicht Stand der Technik. Das soll nicht bedeuten, dass Schätzungen per se nicht angebracht sind. Erfahrene Schätzungen einer Risikohöhe, der Priorisierung oder Zusammenhänge sind eine wirtschaftliche, wenn auch nicht wissenschaftliche Methode!

$Erfahrung$ Die Beurteilung von Korrelationen mittels einer vereinfachten Korrelationsmatrix, die nur Einträge gleich 1 oder 0 zulässt, kann maximal als Grundgerüst für eine künftige Erweiterung dienen. Der Mehrwert, die am meisten vernetzten Risiken zu finden, wird vom Nachteil geschmälert, dass bei Zulassung von mehrfacher Zuordnung, die Gesamtrisikohöhe permanent überschätzt wird, weil ausschließlich volle Korrelationen mit (1) vergeben werden. Bei ausschließlich einfacher Zuordnung entsteht kein Nutzen, denn die Aggregierung erhielte dann nur den quadratischen Mittelwert aller Risiken als Ergebnis.

$Erfahrung$ Letzten Endes muss auch der generelle Umfang und Nutzen von Methoden zur Risikoberechnung kritisch hinterfragt werden. Hat das Unternehmen schon einen entsprechenden Reifegrad um komplexe Quantifizierungen vorzunehmen und im Management Sinn stiftend anzuwenden?

$Erfahrung$ Bei mittelgroßen Nichtfinanzunternehmen sind die Nichtfinanzrisiken in der Realität die Relevantesten. Die Finanzrisiken sind bei konservativer Finanz- und Investitionsführung überschaubar. Vorteile sind z.B. traditionell hohes Eigenkapital, viel Erfahrung im Nischenmarkt, etablierter Firmenhauptsitz und verhältnismäßig kleine Rohstoffmengen. Das Risikomanagement ist dann überwiegend mit strategischen, operativen und betrieblichen Risiken beschäftigt. Die dafür einfachste Methode zur Aggregierung ist die semantische Aggregierung. Diese kann mit einem Ranking der Toprisiken durch Experten, inklusive nochmaliger Beurteilung dieser Toprisiken als Expertenschätzung erfolgen. Alternativ ist das Schätzen der Risiken mit Risikomatrizen inklusive semi-quantitativen Skalen praktikabel.

- **Steuerung:**

$Erfahrung$ Die Mitarbeiter haben während der Workshops bereits zu vielen Problemen Lösungsvorschläge geboten. Diese müssen erfragt und dokumentiert werden.

$Idee$ Eine dem japanischen Kaizen entnommene Methode der Kritikorientierung, Vorschlagswesen für Ideen und Prämierung dieser, erscheint sinnvoll!

$Erfahrung$ Die Steuerung scheint große Ähnlichkeit mit dem Projektmanagement aufzuweisen, daher wird empfohlen auch Methoden von dort zu übernehmen.

$Idee$ Ein Krisenmanagement als mögliche Methode für Toprisiken erscheint sinnvoll. Um schnell reagieren zu können beinhaltet dies Szenarien und deren ausgearbeitete Lösungen. Durch breitgefasstere Krisenpläne ist auch möglich, sich dadurch auf unbekannte Risiken vorzubereiten!

$Problem$ Die Früherkennung, wird allerorts gefordert, da sie genügend Zeit zum reagieren ermöglichen soll. Für die meist nur schwach vorherrschenden Signale scheint dies durch ihren notwendigen Reifegrad an IT-Struktur, Daten und Risikokultur, noch nicht Stand der Technik zu sein!

- In der **Kontrolle und Überwachung** wurden durch die Einführung noch keine eigenen Erfahrungen gesammelt.

$Idee$ Tägliche Risikoberichte mit automatisierten und aktualisierten Risikobewertungen, wie in der Bankwelt üblich, erscheinen für die Risikomanagement Reifegrade der meisten Industrieunternehmen derzeit schwer möglich. Periodisch, zum Beispiel pro Quartal, ist dies aber notwendig.

$Ergebnis$ Die Festlegung einer schriftlichen Risikopolitik und einem daraus abgeleiteten Limitsystem ,ist für die Kontrolle wichtig.

$Problem$ Eine klare Aufgabenzuordnung im Risikomanagement und insbesondere Aufgabentrennung bezüglich der Risikoüberwachung scheint vor allem bei kleineren Unternehmen ungewohnt. Haben die meisten Mitarbeiter doch mehrere Aufgaben und Funktionen. Mindestens nötig ist die Bestimmung eines Gesamtsystem-Verantwortlichen und die Trennung zwischen Risikomanagement und interner Revision.

$Idee$ Im Risikomanagement sind die Workshops, Diskussionen und Gespräche wichtiger als die Berichte!

$Idee$ Ein vorzüglicher Risikoreport findet sich im annual-report der UBS im Kapitel “Risk, treasury and capital management” [4].

- **Einführung eines Informationssystems:**

$Problem$ Eine Verbindung zwischen Risikomanagement und der Unternehmenssteuerung mit bestehenden Organisations-, Planungs- und Berichtssystemen (insbesondere Controlling, balance-score-card, Qualitätsmanagement System) wird allseits gewünscht. Ebenso die Integrierung der Risikoprozesse in die vorhandenen Prozesse. Der Aufwand ist enorm und sollte gut durchdacht werden!

$Ergebnis$ Eine vollständige und verständliche Dokumentation ist im Risikomanagement als Beweislastumkehr und für die Zusammenarbeit vieler Mitarbeiter nötig. Diese ist im besten Fall IT-gestützt.

$Ergebnis$ Neben den Kosten des Risikomanagements, stellt nach [Popescu(2014), F.27] ,vor allem die Überwindung des Silodenkens eine große Herausforderung dar. Das heißt die Überwindung der jeweils eigenwilligen Kriterien-, Risiken- und Reportingwünsche der Abteilungen durch Standardisierungen. Dabei sind Redundanzen in Datenbanken, Prozessen und Systemen zu vermeiden, solange es die Komplexität zulässt.

  – Im letzten Schritt wurden die Daten für die Implementierung in ein IT-System aufbereitet und mit den passenden Dimensionen und Attributen verknüpft. Dies bedurfte 2 intensive Arbeitsmonate in Zusammenarbeit mit dem Softwareunternehmen.

[4] `https://www.ubs.com/global/en/about_ubs/investor_relations/risk.html` (20.06.2015)

  - Als Folgeprojekt muss dieser Risikomanagementprozess nun regelmässig wiederholt werden.

- Als unverzichtbare Quelle für die Entwicklung und Verbesserung eines Risikomanagementsystems sei die **weiterführende Literatur** in Abschnitt 2.3 ausdrücklich empfohlen!

4.9 Nationale und internationale Studien über das Risikomanagement

Es gibt eine Vielzahl von Studien über den Zustand des Risikomanagements in Unternehmen, siehe [accenture(2011)], [pwc(2011), Abb.1], [KPMG and EIU(2013)], [bdi and pwc(2011)], [Olsen et al.(2011)Olsen, Plaschke, and Stelter], [Reiß and Reker(2011)], [McNish(März 2013)], u.v.m.

Bezüglich rein österreichischer Studien, kann man an der Johannes Kepler Universität Linz fündig werden, unter anderem bei [Sitterli(2012)], [Pichler(2002)], [Bokesch(2012)] und [Silbermayr(2012)].

Die relevanten Ergebnisse dieser Studien sind in den Kapiteln dieser Arbeit eingearbeitet und werden hier nicht erneut aufgelistet. Auf den folgenden Seiten wird eine Arbeit über Familienrisiken kurz zusammengefasst, da sie nicht im Internet zugänglich und für viele deutschsprachige Klein- und Mittelständische Unternehmen (KMU) relevant ist. Und im darauffolgenden Abschnitt 4.9 findet man eine Zusammenfassung, die das Risikomanagementsystem eines Beratungsunternehmens als alternativen Zugang erklärt.

Studie zur mittelständischen Unternehmenslandschaft und Familienrisiken

Die Relevanz der KMU im deutschsprachigen Raum steht außer Frage. Der unter Familieneinfluss stehende Anteil an Unternehmen mit über 50 Mitarbeitern ist in Österreich 45%, der Schweiz 75% und in Deutschland bei Unternehmen mit über 50 Mio. EUR Umsatz ein Anteil von 49%. Zusätzlich sind in Österreich 12,5% der Großunternehmen unter Familieneinfluss [Maissner(2010), S.2-3.].

Laut Maissner, die Familienstudien zusammenführte und selbst strukturierte Interviews mit sechs KMUs und sieben Wirtschaftsprüfern führte, sind spezifische Risiken in Familienunternehmen unter anderem [Maissner(2010), S. 36-48]:

- **Management von Familienunternehmen**
  - Die Nachfolgeregelung kann zur Zerreißprobe werden, so ist bei den österreichischen Familienunternehmen nur jedes fünfte in dritter und jedes zehnte in fünfter Generation geführt. Beispiele für Zerreißproben wären mangelnde Bereitschaft zur rechtzeitigen Übergabe oder an unqualifizierte Nachfolger.
  - Streit unter den Gesellschaftern bzw. der Familie, häufig durch Unstimmigkeiten bei Strategie, Gewinnverwendung oder Führungsansprüchen.

  - Nepotismus, also die bewusste Bevorzugung von Verwandten oder loyalen Mitarbeitern gegenüber höher qualifizierten Externen.
  - Keine unabhängigen Experten und unabhängige Gremien zu haben.
  - Unterentwickeltes Controlling oder unterentwickeltes kritisches Bewusstsein.
  - Zu hoher Familienanteil in Unternehmensführung und das Problemfeld Spitzenmanager für Familienunternehmen zu finden, da es generell unter Spitzenmanagern als unattraktiv gilt.

- **Finanzierung und Kapitalstruktur von Familienunternehmen**

  - KMU bevorzugen bei der Finanzierung die Innen- gegenüber der Außenfinanzierung. Bei der Außenfinanzierung wiederum wird Fremdkapital vor Beteiligungskapital gewählt.
  - Der Unabhängigkeitsdrang führt zu überdurchschnittlich hohen Eigenkapitalquoten. Eine Überfinanzierung birgt ebenso wie eine Unterfinanzierung Gefahren, zum Beispiel ungenutzte bzw. verlangsamte Wachstumspotentiale gegenüber jenen die mit Fremdkapital realisiert worden wären.
  - Weiteres Risiko bei hohem Eigenkapitalanteil ist, dass dieser einem Eisberg gleich, finanzielle Alarmsignale überdecken kann, z.B. steigende Kosten und sinkende Rentabilität.
  - Problematisch bei Krisenzeiten ist, wenn Familien ihr gesamtes Vermögen in das Unternehmen investiert haben und keine privaten Reserven zur Absicherung der Familie oder für frisches Eigenkapital haben.
  - Liquiditätsgefährdung durch spezielle familienbezogene Ereignisse wie Ehescheidungen, Erbansprüche, Todesfälle oder Abfindungsansprüche von ausgeschiedenen Gesellschaftern.

Reale Risikoprozesse bei Familienunternehmen scheinen sehr inhomogen zu sein [Maissner(2010), Kp. 7.4 und S.109-113] und zeigen einmal mehr, dass Unternehmen bei der Installation eines Risikomanagementsystems auf ihre eigenen Bedürfnisse eingehen können. Bewährt für Familien hätten sich Familienräte und sogenannte Familienverfassungen, siehe Tabelle 4.10. Lösungen für große Familienunternehmen können organisatorische Maßnahmen wie ein Familienbüro oder spezielle Ausbildungen für Familienmitglieder sein.

Dass Familienrisiken wie Unternehmensnachfolge auffällig selten genannt werden, kam auch bei einer groß angelegten Studie 2011 [bdi and pwc(2011)] zum Vorschein. Nur 19% der KMU und 3% der Großunternehmen (über 1 MRD EUR) gaben dieses Risiko an, obgleich in den Jahren bis 2016 rund ein Viertel der deutschen Familienunternehmen einen Eigentümerwechsel vollziehen werden.

Präambel	• Konsensformen • Selbstverpflichtung • Motto
Werte	• Familien- und Unternehmenswerte • Unternehmensprägung
Ziele	• Familien- und Unternehmensziele • Vermögensziele • Rendite-, Dividenden- und Wachstumserwartungen
Rollen	• Beteiligungsverhältnisse • Familien- bzw. Fremdmanagement • Voraussetzungen für Familienmitglieder zur aktiven Mitarbeit im Unternehmen • Rechte und Pflichten von Familienmitgliedern
Institutionen	• Familientreffen und -versammlungen • Familienrat • Family Office
Anhang	• Fairnesskodex • Verhaltenskodex • Leitlinien • Umgang mit Konflikten und Konfliktlösungsmechanismen • Regeln zur Informationsversorgung aus dem Unternehmen

Tabelle 4.10: exemplarischer Aufbau einer Familienverfassung [Maissner(2010), Tab. 3]

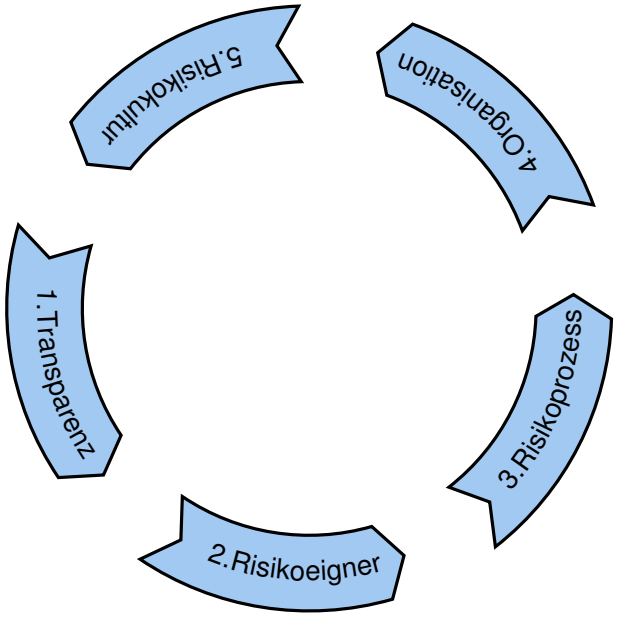


Abbildung 4.19: McKinsey Framework für ein unternehmensweites Risikomanagementsystem mit Befähigungen [McNish(März 2013), Exhibit 3]

Aufbau und Reifegrad eines Risikomanagementsystems aus Sicht einer Unternehmensberatung

In der Bewertung der Reife von Risikomanagementsystemen gibt es viele Ansätze, siehe Abschnitt 3.3. Viele große Unternehmensberatungen haben einen geringfügig abweichenden, eigenen Ansatz entwickelt. Stellvertretend hierfür zeigt Abbildung 3.3 die Bewertungskomponenten des unternehmensweiten Risikomanagementsystems nach McKinsey [McNish(März 2013), Exhibit 4]. Dieses Modell wurde augenscheinlich für Großkonzerne entwickelt und fasst Erfahrungen aus dem Finanzbereich zusammen. Aufgrund der Detailfülle wird dies nicht für einen industriellen Mittelstandsbetrieb gewählt, sondern dient hier als Anregung.

Nach [Pergler(Dezember 2012), S. 2] werden die Reifegrade in vier Stufen definiert und wie bereits einleitend erwähnt, haben gerade eine Handvoll Investmentbanken oder Rohstoffförderer das Level drei von vier. Regionalbanken oder Telekoms sind Beispiele für das Level 1 und forschungsintensive oder risikoreiche Unternehmen für Level 2. Für die nach [Pergler(Dezember 2012), S. 2] befragten Unternehmen waren die beiden kritischsten Bereiche die Datenaufbereitung und übersichtliches Reporting. Ein weiteres Benchmark von McKinsey ermittelte die Risikokultur als kritischsten Punkt [McNish(März 2013), Exhibit 5].

1. **Initiale Transparenz**, dabei werden Risiken je nach Gelegenheit opportunistisch behandelt. Als Ergebnis werden regulatorische Mindeststandards eingehalten und regulär auftretende Risiken behandelt.

2. **Systematische Risikoreduktion** mit Hilfe einer Risikolandkarte bzw. -matrix. Das hierfür nötige professionelle Risikomanagement vermeidet unerwartet hohe Ausfälle und bringt Stabilität in die Wachstumsziele des Unternehmens.

3. **Risk-return-management** verwendet quantifizierende Risikokennzahlen wie etwa VaR (value-at-risk) zur systematischen Szenarioanalyse der Gewinne und Verluste. Notwendig wird dies durch Wettbewerbsdruck oder ROE (return-on-equity) Systemen im Unternehmen.

4. **Risikomanagement als Wettbewerbsvorteil**, benötigt eine starke Risikokultur wodurch eine aktive Risikobehandlung entsteht. Die Unternehmensleitung nutzt risikoadjustiertes Performancemanagement und nutzt Risikomanagement bei der Entscheidungsfindung wie z.B. von Nischenmärkten.

Das unternehmensweite Risikomanagementsystem wird erst erfolgreich, wenn alle Befähigungen nach McKinsey Abbildung 4.19 erfüllt werden können, also einen entsprechenden Reifegrad aufweisen. Die fünf Befähigungen im Risikomanagement können weiters nach Abbildung 4.20 untergliedert werden.

Im Detail wurden folgende Beobachtungen zu jeder Befähigung im Risikomanagement gemacht [McNish(März 2013), S.4ff]:

1. **Risikotransparenz und -einblick** bedeutet im Kern, dass ein breites Risikoverständnis sowohl in fachlicher Natur bei den täglichen Aufgaben als auch über den unternehmensweiten Nutzen des Risikomanagements herrscht.

   IST: Zurzeit werden meist nur einzelne quantifizierbare Risikoarten in einzelnen Abteilungen betrachtet und alle dafür vorhandenen historischen Daten herangezogen.

   SOLL: Künftig soll eine unternehmensweite Risikobeurteilung stattfinden, die auch qualitative Risiken (Reputation- oder Rechtsrisiken) mit einbezieht. Die vorherrschenden ex-post Betrachtungen sollen sich zu Echtzeit- oder ex-ante Vorhersagen entwickeln. Dafür können Stresstest-Methoden und IT-Systeme am modernsten Stand dienen. Gut strukturierte und unternehmensspezifische Risikokataloge die rigoros alle Risiken aufschlüsseln und in Kategorien einteilen. Diese sollten die Risiken auf einzelne Unternehmensbereiche unterteilen und wieder aggregieren können.

2. **Risikoeigner, -appetit und -strategie** in ausformulierter Form. Verwendung von messbaren Kennzahlen und Methoden für die Aggregierung je nach Unternehmensstufe.

   IST: Kennzahlen für den Risikoappetit und passende Limitsysteme sind immer noch eine Herausforderung.

   SOLL: Eine Balance zwischen allgemeinen unternehmensweiten Kennzahlen und individuellen Bereichskennzahlen durch parallele Prozesse mit top-down (Unternehmensleitung) und bottom-up (Mitarbeiterworkshops) sollte gefunden werden.

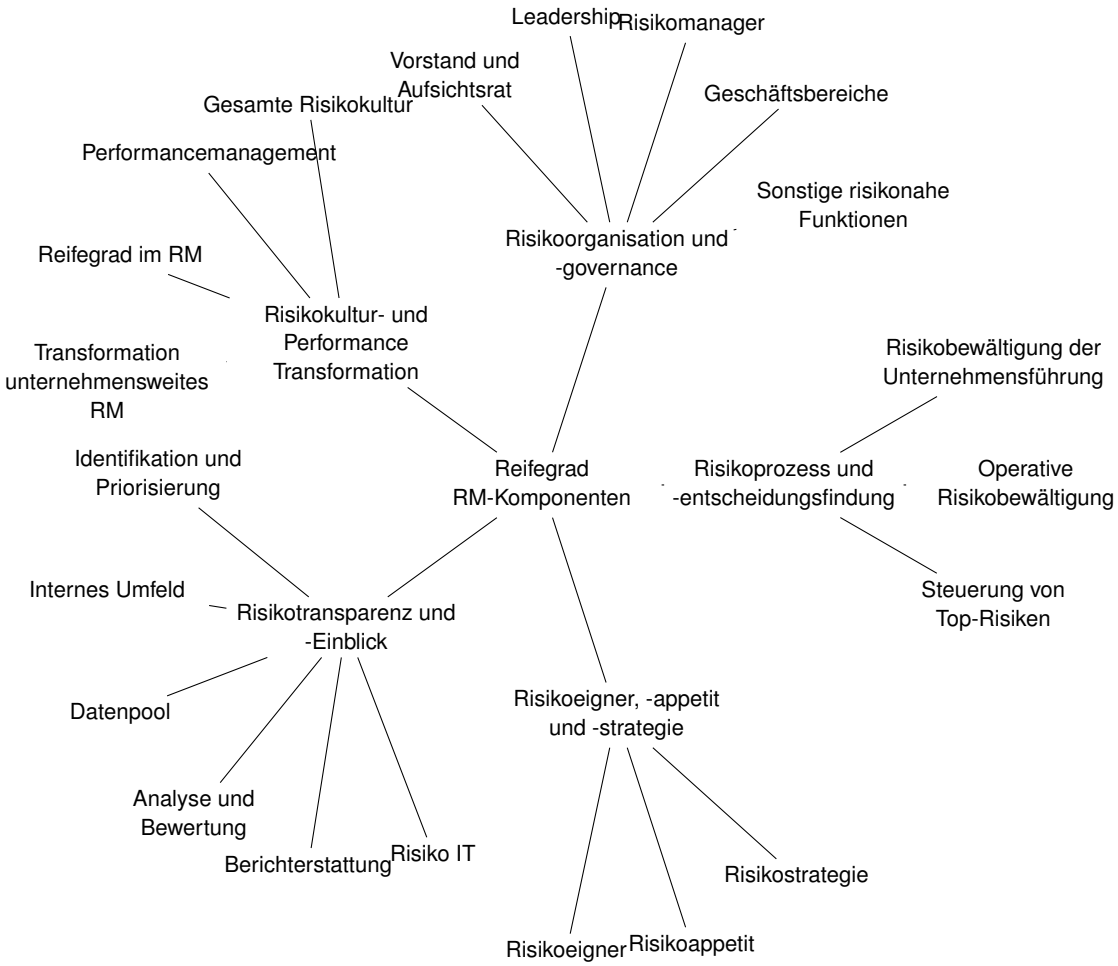


Abbildung 4.20: Reifegrad der Risikomanagementsystem Komponenten [McNish(März 2013), Exhibit 4]

Softe Risiken, welche nicht quantitativ geschätzt werden können, werden mit qualitativen Kennzahlen beschrieben oder geschätzt. Regelmäßige Prozessreviews und -audits stellen sicher, dass die relevantesten Unternehmensbereiche mit hohem Risiko oder Wachstum am gewissenhaftesten betreut werden.

3. **Risikoprozess und -entscheidungsfindung** sind im ganzen Unternehmen eingebunden.

   IST: Die Risikotragfähigkeit und das Restrisiko sind bei Finanzunternehmen seit der 2008 Finanzkrise etabliert.

   SOLL: Gesamtrisiken werden auf Portfolioebene täglich aggregiert und beeinflussen strategische Entscheidungen, Kontrolltätigkeiten und eine robuste Liquiditätspla-

nung. Eine Risikokultur nach Abschnitt 3.3, die einen vernünftigen und transparenten Risikoanreiz schafft.

4. **Risikoorganisation und -governance** für die Verantwortlichkeiten, den tone-at-the-top, Organisationsstruktur und Bürokratisierung.

   IST: Selbst bei vorhandenen Risikomanagern oder Risikovorständen, bestehen oft starke Unterschiede auf den verschiedenen Unternehmensebenen und Schwierigkeiten dies zu aggregieren.

   SOLL: Die Unternehmensführung legt eine Priorität auf das Risikomanagement als Kernfunktion und Abteilungen sind engagierte Risikoeigner mit Expertenpools.

5. **Risikokultur- und Performance Transformation** für die vorherrschende Mentalität und Unternehmenskultur.

   IST: Unternehmen sind sich über die Wichtigkeit der Risikokultur bewusst, es fehlt jedoch an passenden Messgrößen und Veränderungsmethoden.

   SOLL: Engagiertes Risikokultur Programm mit eigener Vollzeitposition im Risikomanagement.

Die daraus abgeleiteten Unternehmenspraktiken sind folgende [McNish(März 2013), S.8ff]:

- Nach Einschätzung entwickelt sich das Risikomanagement zu einer Komponente im Entscheidungsprozess der Unternehmensführung als Erweiterung der bisher vorherrschenden Regulations- und Kontrollfunktion. Bisher spiegelt es sich meist noch nicht im gelebten Unternehmensalltag wider.

- Jedes Unternehmen muss seine ihm eigenen inhärenten Risiken angepasst an den eigenen Fähigkeiten behandeln und in aggregierter Form mit dem Risikoappetit abgleichen.

- Strategisches Risikomanagement zielt auf Compliance Einhaltung, Schadenslimite, Profitabilitätsgewinn, Unterstützung für Wachstumssegemente, Qualitätssteigerung bei Unternehmensentscheidungen, Stakeholder Management und der bewussten Anpassung der Unternehmenskultur ab.

- Operativ wird das Risikomanagement als Prozess aufgefasst, welcher von einer Risikostrategie, -kommunikation, -beurteilung, -kontrolle, -governance bis zur Compliance reicht.

- Die Transformation in ein unternehmensweites Risikomanagement braucht mindestens ein Jahr. Gleich zu Beginn sollte eine Prioritätenliste mit konkreten schnellen Erfolgen erstellt werden, um die breite Akzeptanz im Unternehmen zu steigern.

- Durch die Transformation in ein unternehmensweites Risikomanagement, das über die gesetzliche Notwendigkeit hinaus geht, werden Verbesserungen im strategischen Management, risikoadjustierte Kosten, Stakeholderbeziehungen oder kosteneffizientes Risikomanagement erzielt.
- Es gilt als unwahrscheinlich, dass es jemals einen universal gültigen Zugang zum Risikomanagement geben wird. Ein strukturierter Zugang, jenseits der simplen Betrachtung einzelner Risiken, ermöglicht eine transparentere und risikoabwägende Umsetzung der Unternehmensstrategie.

Eine weitere McKinsey Studie überträgt und verallgemeinert die Risikomanagement Erfahrungen aus der Finanzbranche auf Unternehmen [Pergler(Dezember 2012), S.1ff] und gibt folgende Ratschläge:

- Industrieunternehmen haben aus der Arbeitssicherheit und funktionalen Sicherheit bereits Erfahrungen mit dem operativen Risiken gesammelt. Diese sind nicht immer mit denen der Finanzdienstleister zu vergleichen, da sie Spezialisten für Markt- und Kreditrisiken sind und das Risikomanagement deren Kernaufgabe darstellt.
- Durch diese Unterschiede und der derzeitigen Orientierung des unternehmensweiten Risikomanagements an der Finanzindustrie, nehmen Industrieunternehmen dies meistens als unspezifisch, bürokratisch, ineffizient oder stark verzögernd wahr.
- Die Ziele des Risikomanagements sinds eine Existenzsicherung des Unternehmens, durch deren robusten Aufbau und erhöhte Flexibilität.

Teil III

Risikomanagement Informationssystem in Theorie und Praxis

KAPITEL 5

Grundlagen über Informationssystem

Das beiliegende Kapitel erklärt die grundlegenden Konzepte des IT-gestützten Risikomanagements wie es in einem mittelständischen Konzern zur Anwendung kommt. Da es sich um Grundlagen handelt, ist dieses Kapitel unabhängig von der tatsächlich verwendeten Software-Lösung gültig und gilt sowohl für integrierte als auch alleinstehende IT-gestützte Risikomanagementsysteme.

Nach einer Erklärung der Anwendungssysteme als der automatisierte und softwareunterstützte Teil des Informationssystems, erfolgt eine Einteilung in analytische und operative Anwendungssysteme, siehe Abschnitt 5.1. Dabei wird das Informationsmanagement nach dem dreiteiligen Modell von Krcmar aufgebaut.

Bei der Beschaffung eines IT-Systems ist stets die Entscheidung zu treffen, ob ein Standard-System ausreicht oder ein individuelles System nötig ist. Deren Vor- und Nachteile und die Entwicklungsanforderungen sind zu bedenken. Gängige Risikomanagement Software Anbieter und das passende Gartner Benchmark werden in Abschnitt 5.1 vorgestellt. Für den Fall, dass eine Eigenentwicklung in Betracht gezogen wird, zeigt Abschnitt 5.2 die verschiedenen fachlichen Disziplinen, einen ingenieurmäßigen Entwicklungsprozess und Qualitätskriterien. Sowohl als Standard-System als auch bei Eigenentwicklung verursacht die Integration eines neuen Systems in ein Unternehmen 30-50% der Gesamtkosten. Die Integration kann prinzipiell auf zwei Weisen erfolgen, als Verknüpfung der Datenbanken oder der IT-Prozesse.

Der Abschnitt 5.3 erklärt die 3-Schichten-Architektur eines Anwendungssystems. Darauf folgend hat jede Schicht ein eigenes Kapitel. Die Datenbankschicht erklärt die Erstellung eines Datenmodells mittels Relationenmodell und die generelle Handhabung von Daten. Die Verarbeitungsschicht dient der Datenanalyse mittels mehrdimensionalen Kennzahlen

(OLAP) und gibt führende business-intelligence Anbieter an. Die Präsentationsschicht geht auf die Prinzipien der Benutzerschnittstellen bzw. -oberflächen ein.

5.1 Einführung in softwareunterstützte Informationssysteme

Die Bedeutung von Informationssystemen wird in der Beschreibung der einzelnen COSO II Komponenten ersichtlich, so weist bereits das interne Umfeld auf den gegenseitigen Einfluss von IT- und Risikomanagement hin [COSO(2006), vgl. S.27ff]. Insbesondere die Kontrollaktivitäten verlangen eine angemessene Kontrolle über die im Risikomanagement verwendeten Informationssysteme [COSO(2006), vgl. S.55ff]. Die Komponente Information und Kommunikation handeln größtenteils über Funktionen eines Informationssystems, die für ein effektives Risikomanagementsystem benötigt werden [COSO(2006), vgl. S.67ff].

Beim Informationsmanagement spielt die Integration von verschiedenen IT-Systemen in einem Unternehmen eine entscheidende Rolle. Dies kann auf zwei Weisen erfolgen. Durch Verknüpfung verschiedener Datenbestände, der sogenannten Informationsintegration (auch -fusion, -konsolidierung oder data-warehousing genannt), oder durch Anwendungsintegration bei den IT-Prozessen. Laut Schätzungen sind über 50% der IT-Kosten durch die Integration verursacht, daher ist dieser Punkt frühzeitig in der Planung zu berücksichtigen. [Leser and Naumann(2007), S.3]

Ein Informationssystem und dessen Kennzahlen brauchen die richtige Informationslogistik, sonst gilt: "junk data in is junk data out".

Die Planung, Steuerung und Überwachung von Informationen unterliegt der Informationslogistik als Teilgebiet des Informationsmanagements. [Schwarzer and Krcmar(2014), S.10] [Abts and Mülder(2013), S.10]: Das bedeutet, dass die richtige Information, in richtiger Form, zur richtigen Zeit und beim richtigen Mitarbeiter verfügbar ist. Dieses Prinzip wurde aus den klassischen Zielen der Logistik abgeleitet, die die richtigen Objekte, in den richtigen Mengen, in der richtigen Qualität, zur richtigen Zeit, zu richtigen Kosten, an den richtigen Ort und mit dem richtigen Ressourcenaufwand bereitstellen sollen. Der betriebswirtschaftliche Vergleich gegenüber Informationen und materiellen Wirtschaftsgütern zeigt die grundlegenden Unterschiede, so haben Informationen keinen Wertverlust durch Gebrauch, kaum Vervielfältigungskosten und eine einfachere Logistik. Informationen haben gegenüber materiellen Gütern jedoch auch schwerere Schutzmöglichkeiten, die Preisbestimmung am Markt gestaltet sich unübersichtlicher und sowohl zu viele als auch zu wenige Informationen sind problematisch [Krcmar(2015), vgl. S.5]:

Das Informationsmanagement folgt in dieser Arbeit dem Modell nach Krcmar und hat als Hauptaufgabe die Ressource Information betriebswirtschaftlich sinnvoll zu steuern. Informationssysteme sind soziotechnische Systeme [Krcmar(2015), S.66], welche als wissensorientierte Unternehmensführung in drei fachliche Ebenen und eine übergeordnete Führungsebene unterteilt werden [Krcmar(2015), S.2]:

- Informationswirtschaft, betrifft das Management von Informationsnachfrage, -angebot, -quellen, -ressourcen und -verwendung.

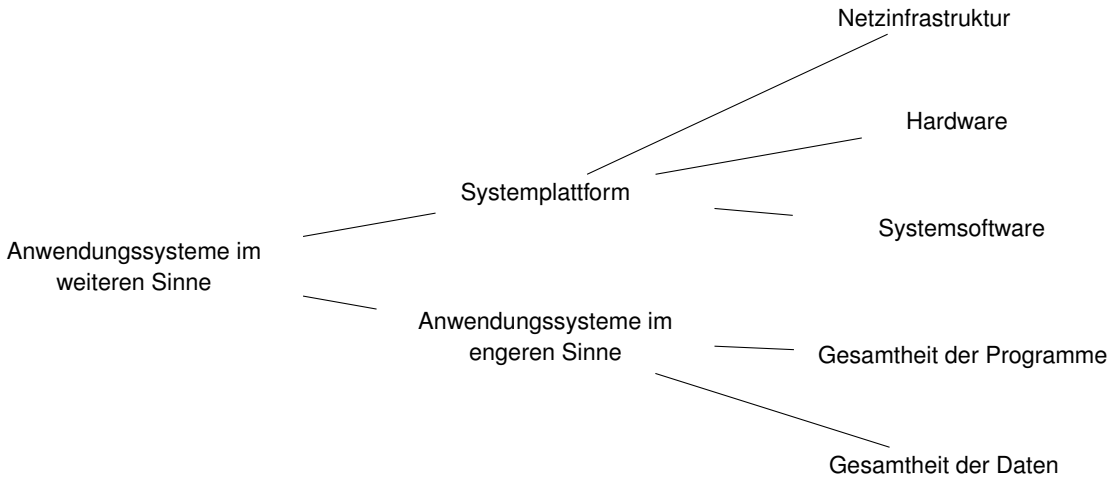


Abbildung 5.1: Anwendungssysteme vgl. [Frick et al.(2009)Frick, Servaes, Abts, Mehrtens, Söhnchen, Mülder, Stegemerten, and Westheide, S. 2ff]

- Informationssysteme, die die Modellierung der Daten und Prozesse beinhalten. Sowie das Management des Anwendungslebenszyklus und der Softwareeinführung.
- und IuK-Technologie (Informations- und Kommunikationstechnik), also technische Basissysteme die Systemaufgaben wie Speicherung, Verarbeitung und Server-Kommunikation übernehmen.
- Die Übergeordneten Führungsaufgaben des Informationsmanagements beinhalten die IT-Governance, -Strategie, -Prozesse, das IT-Personal und IT-Controlling

Das Informationsmanagement ist in der Fachliteratur nicht eindeutig definiert, es überschneidet sich fachlich mit anderen Disziplinen wie dem Wissensmanagement, Dokumentation, Kommunikation, Informationswirtschaft oder Wirtschaftsinformatik.

Anwendungssysteme

In der IT- Praxis werden Informationssysteme oft mit Anwendungssystemen gleichgestellt. Anwendungssysteme bilden den automatisierten Teil eines Informationssystems, denn das Informationssystem schließt die menschliche Komponente noch mit ein. [Schwarzer and Krcmar(2014), S.8]. Die Anwendungssysteme lassen sich im engeren und erweiterten Sinne definieren, siehe dazu Abbildung 5.1.

Die Abbildung Abbildung 5.2 zeigt die historische Entwicklung der Informationssysteme.

- So entwickelten 1965 Großunternehmen systematische Management Informationssysteme zur Berichterstattung ans obere Management. Dies begann mit Großrechenanlagen die periodisch Listen druckten.

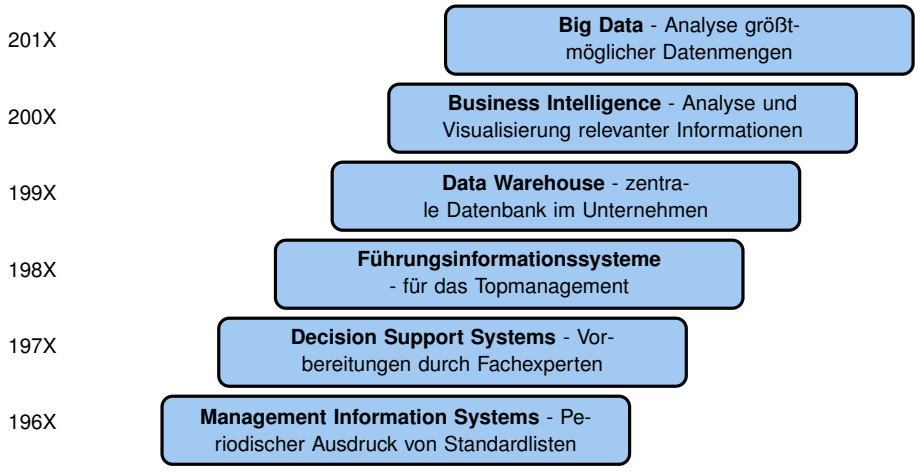


Abbildung 5.2: Weiterentwicklung der analytischen Informationssysteme vgl [Abts and Mülder(2013), S. 266ff]

- In den 70ern wurde unter Nutzung der ersten Tabellenkalkulationsprogramme statistische Simulationen zur Simulation, Prognose und Optimierung durchgeführt und in den ausgedruckten Berichten eingesetzt. Bezeichnet wurde dies als decision-support-system, da diese von Fachexperten aufbereiteten Berichte dem Management als Entscheidungsgrundlage dienten.
- Schließlich konnten in den 80ern grafisch aufbereitete Informationen auf dem ersten personal computer erstellt und vom Topmanagement ohne Hilfe von Assistenten eingesehen werden. Das wurde Führungsinformationssystem (im englischen executive-information-system, bzw. EIS) genannt.
- Seit Mitte der 90er Jahre erkannten viele Unternehmen, dass sich die anspruchsvollen, ständig neuen Informationswünsche des Managements nur durch eine einheitlich strukturierte und dauerhaft verfügbare Datenbank für Kennzahlen und Auswertungen bewältigen lassen, einem data-warehouse.
- Seit den 2000ern ist im deutschsprachigen Raum auch die business-intelligence (BI) etabliert, darunter versteht man die Sammlung, Aufbereitung und Darstellung entscheidungsrelevanter Informationen für Planung, Kontrolle und Steuerung eines Unternehmens. Dabei handelt es sich um einen integrierten und unternehmensspezifischen Gesamtansatz zur Managementunterstützung.
- Seit den 2010er Jahren sind auch große Datenauswertungen aufgrund von Serverfarmen und in-memory am PC (Nutzung des RAM Speicher) gängige Praxis. [Abts and Mülder(2013), S.266ff]

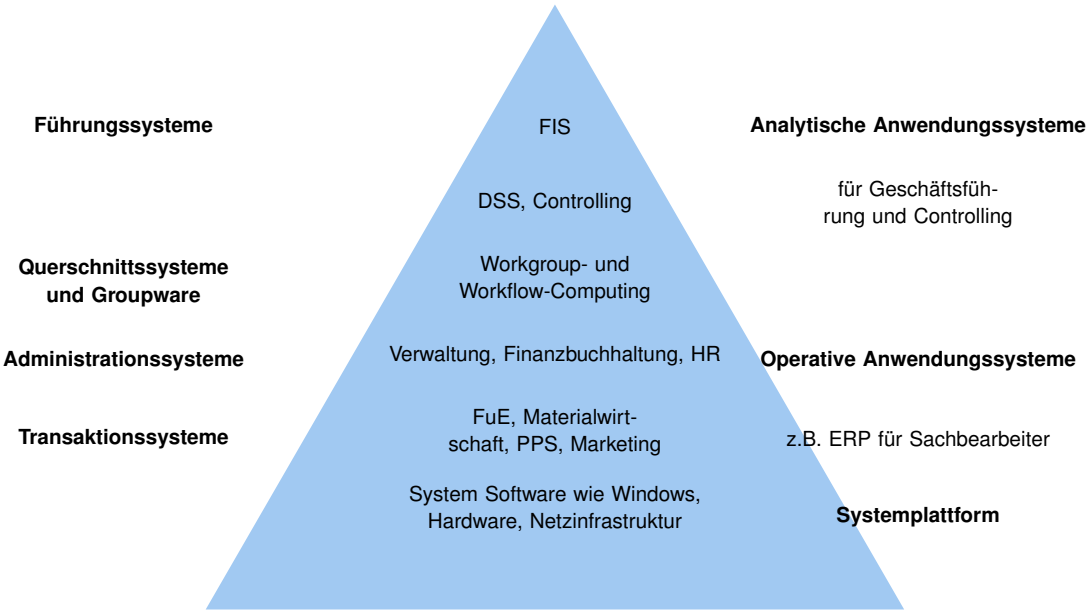


Abbildung 5.3: Übersicht der Anwendungssystemkomponenten in der Pyramide und daneben zwei Einteilungsmöglichkeiten vgl. [Schwarzer and Krcmar(2014), S. 12ff]

Einteilung in operative und analytische Anwendungssysteme

Anwendungssysteme werden in der Wirtschaftsinformatik in analytische Anwendungssysteme, die auch Planungs- und Kontrollsysteme genannt werden und in operative Anwendungssysteme unterschieden, siehe Abbildung 5.3. Operative Anwendungssysteme unterstützen das tägliche Geschäft der Nutzer in den diversen Unternehmensabteilungen. Sie sind somit der Teil der Anwendungssysteme, die nicht nur der IT-Spezialist zu sehen bekommt, sondern fast jeder Nutzer. Weiters können Anwendungssysteme auch nach Verwendungszweck oder Branchen eingeteilt werden [Frick et al.(2009)Frick, Servaes, Abts, Mehrtens, Söhnchen, Mülder, Stegemerten, and Westheide, vgl. S.3], dies wird hier im Detail unterlassen. Beide, operatives und analytisches Informationssystem, sind miteinander verbunden. So versorgt das operative Informationssystem das analytische Informationssystem mit Daten und das Letztgenannte versorgt das Management mit Auswertungen [Frick et al.(2009)Frick, Servaes, Abts, Mehrtens, Söhnchen, Mülder, Stegemerten, and Westheide, vgl. S.268].

Unter Querschnittssystemen versteht man unter anderem Workflow-, Dokumentations- und Wissensmanagement oder Konferenzsysteme.

Missverständnisse bei Informationssystemen können durch eine fehlende einheitliche Definition im Unternehmen und die in der Fachliteratur vielen ähnlichen Spezialsysteme entstehen. Eine detaillierte Untergliederung und Unterscheidung von MIS (Managementinformationssystem), DSS (decision-support-system), EIS (executive-information-system), MSS (Managementsupportssystem) oder ERP (enterprise-ressource-management) wird in

dieser Arbeit nicht weiter unternommen.

Standard IT-Systeme gegenüber individuellen Systemen

Das in dieser Arbeit erschaffene unternehmensweite Risikomanagement Informationssystem beruht auf den gleichen IT-Grundlagen wie jedwedes betriebliche Informationssystem. Insbesondere Industrieunternehmen müssen mit Bedacht auf den Umfang der möglichen Datenquellen, die voraussetzbaren Nutzererfahrungen und generell auf eine Konzeption, die auf die bewährte best-practice zurückgreift, achten. Die speziellen risikobezogenen Unterschiede liegen in den spezifischen Workflows, Datenmodellen und Berechnungsmodellen.

Das zu dieser Arbeit dazugehörende Projekt fokussierte sich nicht auf eine komplette Software-Entwicklung, sondern die Entwicklung eines Risikomanagement Moduls für ein bestehendes Anwendungssystem. Somit entfallen einige Schritte die bei einer vollständigen Neuentwicklung nötig wären.

Anforderungen bei der Entwicklung von Individualsoftware sind, neben einer systematischen und ingenieursmäßigen Vorgehensweise nach [Krcmar(2015), S.67], in Abbildung 5.4 veranschaulicht.

Die elementare make-or-buy Entscheidung, ob eine Standardsoftware nach Abschnitt 5.1 ausreichend ist oder eine Eigenentwicklung nach Abschnitt 5.2 nötig wird, muss im Laufe der Einführung eines Risikomanagements getroffen werden. Nicht zu vergessen ist, dass Standardsoftware ebenfalls einen hohen Implementierungsaufwand hat. Standardsoftware muss im Unternehmen an die jeweilige IT-Systemplattform und fachlichen Prozesse angepasst werden. Standardsysteme haben eine Reihe von Vor- und Nachteilen gegenüber speziell für das Unternehmen entwickelten IT-Systemen [Frick et al.(2009)Frick, Servaes, Abts, Mehrtens, Söhnchen, Mülder, Stegemerten, and Westheide, S.4]:

+ geringere Kosten als bei Eigenentwicklungen
+ Referenzinstallationen von anderen Kunden zeigen deren Tauglichkeit
+ Einführungszeit ist geringer, da die Eigenentwicklungszeit eingespart wird
+ Standardsoftware ist in der Regel ausgereifter und qualitativer
+ Weniger eigenes knowhow ist erforderlich
+ Schnittstellen zu anderen Anwendungssystemen oder Drittanbietermodulen
+ Schulungen und Support werden von externen und eingespielten Spezialisten übernommen
+ hohe Investitionssicherheit
− Das Unternehmen muss sich an die Prozesse der Standardsoftware anpassen und muss somit zu einem gewissen Teil die Risikomanagement Vorstellungen des Anbieters teilen bzw. übernehmen

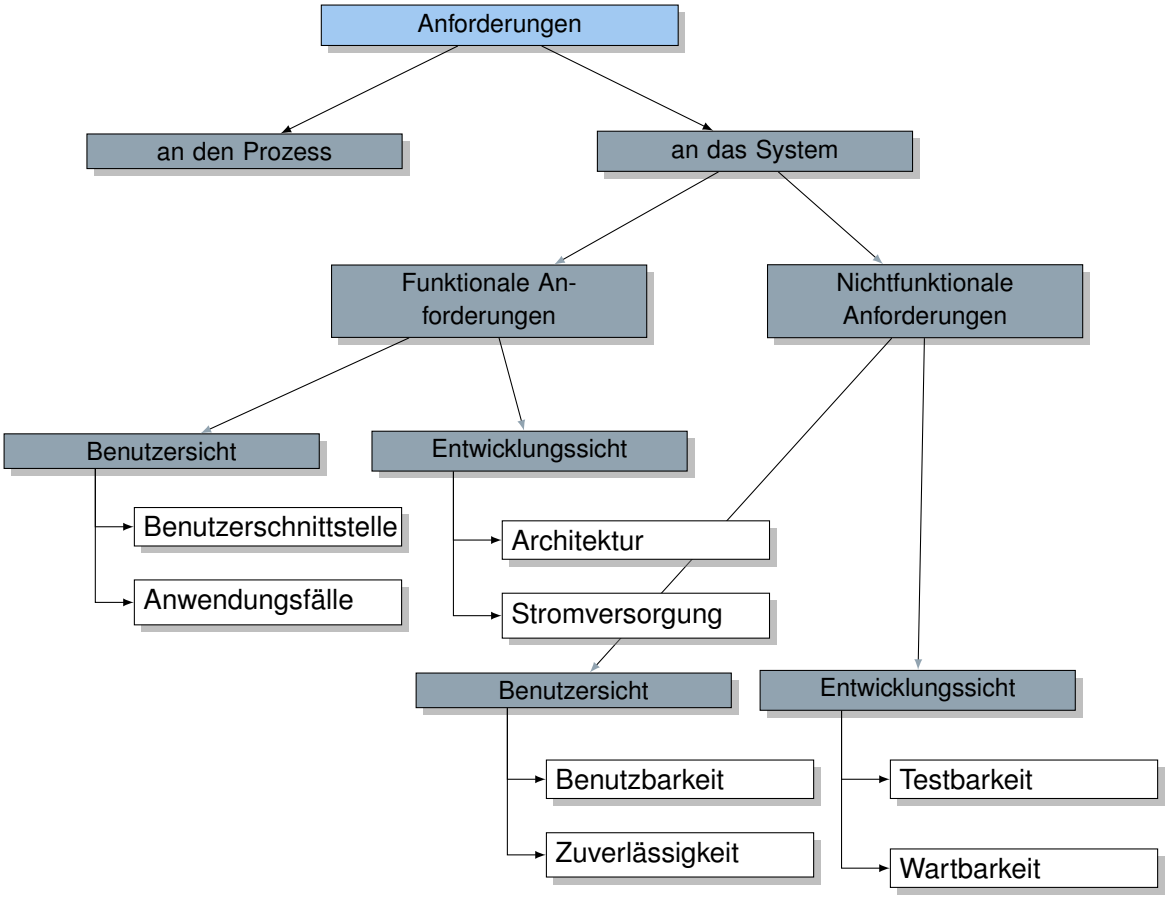


Abbildung 5.4: Unterschiedliche Typen von Anforderungen bei der Entwicklung von Individualsoftware nach [Krcmar(2015), Abb. 3.10]

- Begrenzte und teure Individualisierungen bzw. Anpassungen
- Abhängigkeit vom Anbieter und seinen Betreuungsressourcen
- “lockin” Effekte durch die Implementierung einer Software und dessen Datenbanken.

Ob die Software als Standardlösung gekauft oder selbst entwickelt wird, der Implementierungs- und Testaufwand fällt in beiden Fällen an. Eine gängige Empfehlung im Prozessmanagement lautet, jede Änderung in der Software- oder Prozesslandschaft für eine Optimierung und Aktualisierung der Prozesse zu nutzen, es wäre sonst eine verpasste Chance die veralteten Prozesse zu entstauben [Wagner and Patzak(2015)].

Risikomanagement Software Anbieter

Das Risikomanagement hat mehrere Branchen die eine Vorreiterstellung einnehmen. Im technischen Bereich sind dies im allgemeinen das Qualitätsmanagement oder im Speziel-

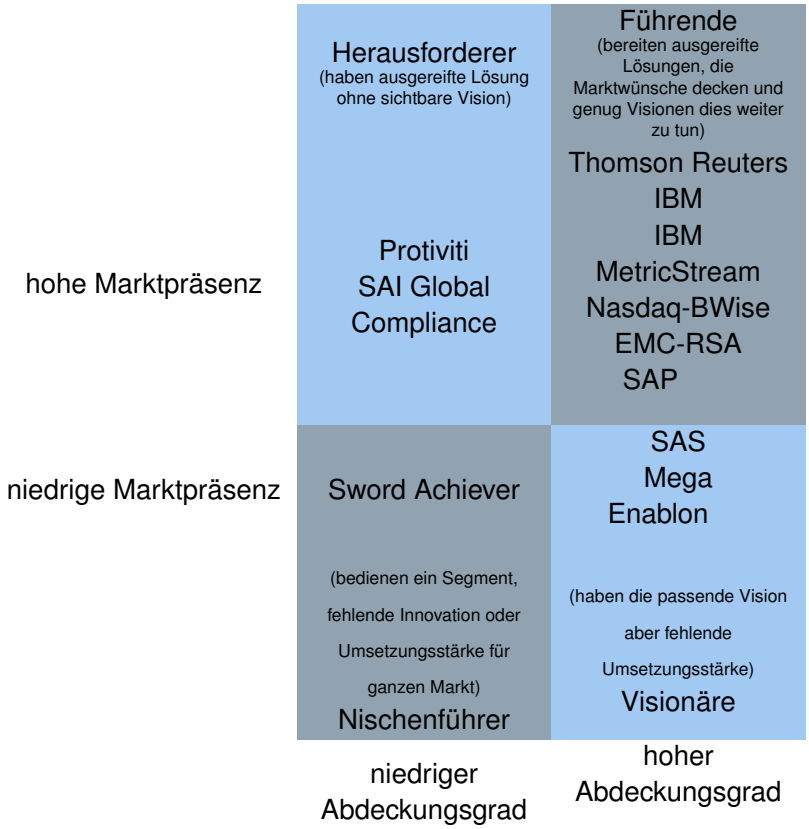


Abbildung 5.5: Gartners “Enterprise Governance, Risk and Compliance Platforms Magic Quadrant” [Gartner(2011), vgl. S.7ff]

len, Methoden aus den sicherheitskritischen Entwicklungen in der Nuklear-, Luft- und Raumfahrttechnik. Im unternehmensweiten Risikomanagement sind vor allem in den letzten Jahrzehnten Regulierungen und best-practices aus der Finanzbranche übernommen worden, siehe Abschnitt 2.2. Dass die Erkenntnisse aus den Vorreiterbranchen nicht eins zu eins in jede andere Branche übernommen werden können, ist naheliegend.

Ein Benchmark der bestehenden Risikomanagement Software am Markt wurde 2014 von Gartner Group untersucht und in ihrem Magic Quadrant Abbildung 5.5 [1] mit den zwei Dimensionen Abdeckungsgrad (engl. completeness-of-vision) und Marktpräsenz (engl. ability-of-execute) verglichen. Diese zwei Dimensionen vermögen es jede kommerzielle Software zu vergleichen und zu ranken [Gartner(2011), vgl. S.7ff].

Die Auswahl von Software ist eine eigene Disziplin in der Informatik und sollte als eigenes Projekt betrieben werden [Abts and Mülder(2013), vgl. S.497ff]. Da Software 7 bis 10 Jahre im Einsatz ist und Informationssysteme aufgrund der Wechselbarrieren noch län-

[1] vgl. `https://www.gartner.com/doc/2595717/magic-quadrant-enterprise-governance-risk` (1.10.2013).

ger, sollte dies folgende Phasen beinhalten: Prozessanalyse, Prozessoptimierung, Anforderungsdefinition, Softwaremarkterhebung, Softwaretest und -auswahl, Vertragsabschluss, Implementierung, Systemabnahme und Einführung.

5.2 Software Entwicklung von individuellen Anwendungssystemen

Disziplinen der Informatik

Die Informatik kann nach mehreren Möglichkeiten gegliedert werden, wie dies in jeder Wissenschaft der Fall ist. [2] Bei computerunterstützten Informationssystemen, dem zentralen Thema dieses Kapitels, siehe Abschnitt 5.1, handelt es sich um ein sogenanntes Anwendungssystem, das mittels Datenbanken und Anwendungssoftware (Algorithmen und User-Interfaces) Informationen speichert, auswertet und aufbereitet. Es unterliegt somit den gleichen Entwicklungsmethoden und Kundenanforderungen wie jede Software [Gumm and Sommer(2013), S.2].

Software Engineering ist die Anwendung eines systematischen, konsequenten, quantifizierten und somit ingenieurswissenschaftlichen Ansatzes für die Entwicklung, Betreibung und Wartung von Software. Die ingenieursmäßig sinnvollste Unterteilung der Computer Wissenschaften nach Radinger verwendet folgende Disziplinen [Radinger(2010), F. 10]:

- Theoretische Informatik
- Programmiersprachen
- Betriebssysteme
- Software Entwicklung (Engineering)
- Datenmanagement (Informationsmanagement)
- Künstliche Intelligenz (hier Business Intelligence)

Die Entwicklung eines computerunterstützten Informationssystems für das Risikomanagement bedarf alle dieser Gebiete, im folgenden Kapitel wird speziell auf die Datenmodellierung Abschnitt 5.4, Software Entwicklung Abschnitt 5.2 und Business Intelligence Abschnitt 5.5 eingegangen. Nach diesen Bereichen ist auch der Aufbau dieses Kapitel gegliedert.

Verwendete Methoden während der Softwareentwicklung

Große Software Projektentwicklungen verwenden einen vollständigen und sequenziellen Entwicklungsprozess wie etwa in Abbildung 5.6 [Gumm and Sommer(2013), S.829] gezeigt [3]. Die in der Abbildung verwendeten Schritte sind folgend kurz erklärt:

[2] vgl. http://en.wikipedia.org/wiki/Category:Areas_of_computer_science (17.10.2014).

[3] im Englischen werden gleichbedeutend die Begriffe software-development-process, software-development-livecycle oder software-development-model benutzt

- Hierarchiediagramme zeigen das reale Unternehmen und sind Flussdiagramme wie etwa Arbeitsabläufe oder Organigramme (siehe Abbildung 4.1).

- In der objektorientierten Entwicklung stehen die Abkürzungen OOA für objekt-oriented-analysis, OOD für objekt-oriented-design und OOP für objekt-oriented-programming. Objekte sind Funktionen die das System später erfüllen muss. Während der objektorientierten Analyse (OOA) werden alle nötigen Objekte gesucht, geordnet, beschrieben, Varianten simuliert und deren Anforderung erstellt. Dies kann beispielsweise mittels UML-Diagrammen als object-charts erfolgen. Diese UML Diagramme werden im Zuge des objektorientierten Design (OOD) mit den vorhandenen Prozessen, technischen Systemmöglichkeiten und Benutzerwünschen in Einklang gebracht und anschließend zur Implementierung verwendet [4] .

- UI-Skizzen (engl. user-interface) zeigen prototypisch die künftige Benutzeroberfläche (engl. mock-up), diese können händisch oder per MS-Office erstellt werden und richten sich anhand der vorhandenen oder künftigen Arbeitsabläufe. UID (user-interface-design) bedeutet die Entwicklung der Benutzeroberfläche mittels üblicher Funktionen einer GUI Software (Abkürzung für graphical-user-interface) [Bourque and Fairley(2014), vgl. Kp. 2.4].

- EER steht für extended-entity-relation-diagram und zeigt das gewünschte Datenbankmodell wie in Abschnitt 5.4 erklärt.

Die Abbildung 5.6 ist nur eine Möglichkeit von vielen weiteren Vorgehensmodellen, so verwenden sicherheitskritische Anwendungen z.B. das V- oder Spiral-Modell. Kleinere Entwicklungen genügen den agilen Methoden [Schwarzer and Krcmar(2014), S.153]. Die Kernaktivitäten aller oben erwähnten Modelle sind jedoch immer die Gleichen: Planung, Analyse der Anforderungen, darauf folgend Design, Implementierung, Testung und Inbetriebnahme. Sie sind aus den Prozessen des Lebenszyklus nach ISO/IEC 15288 entnommen [ISO(2008), S. 12 Abbildung 4], [Schwarzer and Krcmar(2014), S.144], [Bourque and Fairley(2014), S. Vff] und [Gumm and Sommer(2013), S.830-832] und gleichen dem kontinuierlichen Verbesserungsprozess des plan-do-check-adjust Modells von W. Edwards Deming.

Dass dabei das Rad nicht immer von neuem erfunden werden muss, versteht sich von selbst. Standardmethoden der Softwareentwicklung sind etwa [Gumm and Sommer(2013), vgl. S.831ff]:

- Ein Projekthandbuch bzw. Projektproposal für die Planungsphase, [Abts and Mülder(2013), vgl. S. 500 und Kp.13.5].

- Requirement Engineering siehe Abschnitt 6.1 und Abbildung 5.4 nach [Abts and Mülder(2013), vgl. S. 507ff] und [Bourque and Fairley(2014), vgl. Kp. 1.7].

[4] https://en.wikipedia.org/wiki/Object-oriented_analysis_and_design (24.07.2015)

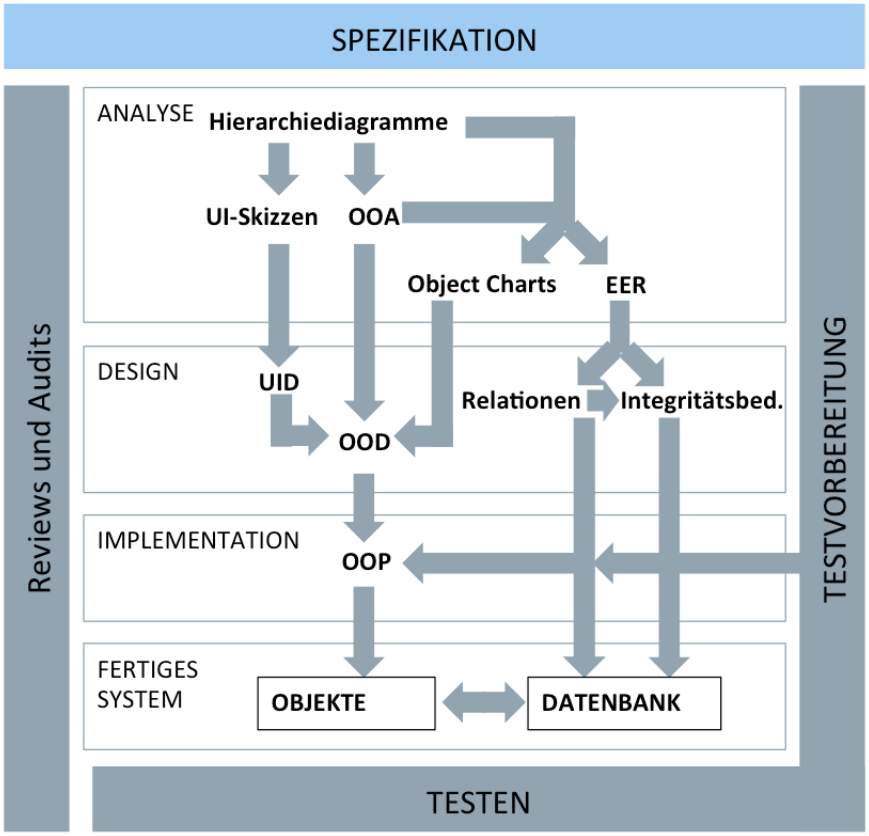


Abbildung 5.6: Softwareentwicklungsprozess anhand [Bourque and Fairley(2014), S.]

- Skizzierte user-cases (dt. Anwendungsfalldiagramm) oder management-activity-diagrams dienen dazu ein Verständnis der realen Prozesse zu erlangen [Abts and Mülder(2013), vgl. S. 490ff].
- Relationale Datenbankmodelle wie in Abschnitt 6.2 erklärt und in Abschnitt 6.2 praktisch gezeigt.
- user-interfaces wie in Abschnitt 5.6 erklärt und Abschnitt 6.2 erstellt [Bourque and Fairley(2014), vgl. Kp. 2.4].

Der Bedeutungsgewinn des Risikomanagements, sowohl in der gelebten Praxis als auch in den gesetzlichen Vorschriften, rechtfertigt einen höheren Entwicklungsaufwand. Dabei müssen die Strukturen, Unternehmenskultur und Branchenrealitäten des jeweiligen Unternehmens spezifisch zum Softwareumfang passen.

Die Vorteile die eine strukturierte, sequenzielle und vollständige Softwareentwicklungsmethode hat, wie in Abbildung 5.6 gezeigt, sind etwa eine langfristige Weiterentwicklungsstrategie und eine Robustheit gegenüber Sicherheit und Funktion.

Deren Nachteile sind gleichzeitig die Begründung für die nicht-sequenziellen Entwicklungsmethoden, wie etwa dem Prototyping oder agilen Methoden. Von diesen agilen Methoden erhofft man sich realitätsnahe und flexible Entwicklungsprozesse, wenig Softwarebürokratie und Trennung zwischen Anwender- und Entwicklerwelt zum gemeinsamen Vorteil [Gumm and Sommer(2013), vgl. S.833].

In diesem Projekt wurde die Prototyping Methode verwendet, da das prototypische Anwendungssystem vor allem für die Erforschung der Risikoprozesse und Kundenanforderungen benötigt wird [Schwarzer and Krcmar(2014), vgl. S.148-151]:

- Beim Prototyping wird eine schnell verfügbare und lauffähige Vorabversion erstellt [Schwarzer and Krcmar(2014), vgl. S.148]. Das ermöglicht gezielt auf Aspekte der Methoden, Datenmodelle und Benutzeroberfläche des Risiko Moduls eingehen zu können. Die funktionstüchtige IT-Plattform wurde vom Partnerunternehmen zur Verfügung gestellt.
- Durch den vorhandenen Prototypen können Nutzer in allen Phasen der Entwicklung mitwirken. Dies erhöht Akzeptanz, Flexibilität und Ergebnisqualtität. [Schwarzer and Krcmar(2014), S.148].

Herausforderungen und Qualitätskriterien für Softwaresysteme

Die Qualitätsfaktoren für Softwaresysteme nach ISO/IEC 25000 haben eine allgemeine Gültigkeit und sind bei jeder Software Entwicklung zu beachten: [Biffl(2010), F. 11] [Schafferer(2011), F. 30]

- Funktionalität mit Korrektheit, Angemessenheit, Interoperabilität, Sicherheit, Ordnungsmäßigkeit, Integrität.
- Zuverlässigkeit mit Reife, Fehlertoleranz (Robustheit), Wiederherstellbarkeit und Compliance im Sinne von Einhaltung rechtlicher Erfordernisse.
- Benutzbarkeit, wie Verständlichkeit, Erlernbarkeit, Bedienbarkeit.
- Änderbarkeit, wie Analysierbarkeit, Wiederverwendbarkeit, Stabilität, Flexibilität, Wartbarkeit, Testbarkeit.
- Effizienz und Effektivität, wie Verbrauchsverhalten und Zeitverhalten.
- Übertragbarkeit, wie Installierbarkeit, Austauschbarkeit, Verknüpfbarkeit, Portabilität.
- Sicherheitsziele nach COBIT ergänzen die Qualitätskriterien mit Vertraulichkeit, Integrität, Verfügbarkeit [ISACA(2012), S.63].

Das Software Qualitätsmodell nach McCall [Biffl(2010), F. 11] gibt messbare Kriterien in der ersten Spalte in Tabelle 5.1 vor. Zusätzlich teilt sie die Kriterien den übergeordneten Qualitätskriterien zu, diese sind in der ersten Zeile gruppiert nach Verwendung.

Verwendung:	Einsatz des Produkts					Produktänderungen			Produktwechsel		
Faktoren:	**Verwendbarkeit**	**Integrität**	**Effizienz**	**Fehlerfreiheit**	**Verfügbarkeit**	**Wartbarkeit**	**Testbarkeit**	**Flexibilität**	**Wiederverwend-barkeit**	**Portierbarkeit**	**Kompatibilität**
Kriterien:											
Bedienbarkeit	x										
Trainierbarkeit, Schulung	x										
Kommunikation	x										
Zugriffskontrolle		x									
Zugriffsüberprüfung		x									
Speichereffizienz			x								
Ausführungseffizienz			x								
Rückverfolgbarkeit				x							
Vollständigkeit				x							
Genauigkeit					x						
Fehlertoleranz					x						
Konsistenz				x	x	x					
Einfachheit					x	x	x				
Übersichtlichkeit, Kürze						x					
Testabdeckung							x				
Instrumentierung							x				
Erweiterbarkeit								x			
Allgemeinheit								x	x		
Selbsterklärend							x	x	x	x	
Modularität							x	x	x	x	x
Hardware-Unabhängigkeit									x	x	
Plattform-Unabhängigkeit									x	x	
Kommunikationskompatibilität											x
Datenkompatibilität											x

Tabelle 5.1: Software Qualitätsmodell nach McCall [Biffl(2010), F. 11]

Die Herausforderungen in der Entwicklung von Software sind seit den 1960er Jahren die Gleichen und ident mit den Qualitätsfaktoren aus Tabelle 5.1.

Folgende Ziele in der Entwicklung von Software sollen dem künftigen Entwickler als Ansporn und Warnung gelten [Hanschke(2013), vgl. Kp. 2.1]:

- Sicherstellung der operationellen Exzellenz
  - Beherrschung und Reduktion der IT-Komplexität durch fortwährende IT-Konsolidierung. Komplexität wird durch Visualisierung des IT-Systems und seiner Schnittstellen sichtbar.
  - Risikomanagement als wichtiger Aspekt der operationellen Exzellenz
- Agilität als Begriff für eine IT die sich auf ändernde Prozesse einstellen kann.
  - Agilität kann als time-to-market gemessen werden, also der Zeitpunkt von der Einführung oder Veränderung bis die Software wieder funktioniert.
  - Dies beinhaltet eine Komponentisierung des gesamten IT-Systems und eine Integrationsarchitektur als Plattform, die diese verbindet.
- IT als business-enabler. Somit soll die IT einen Beitrag an der Wertschöpfung und Erreichung der strategischen Ziele haben.
  - Voraussetzungen für eine steigende Wertschöpfung sind eine unbürokratische und durchsetzbare IT-Strategie, eine passende IT-Organisation und eine klare und effektive IT-Governance in Form von Regeln und gemeinsamer Sprache im Unternehmen .
  - IT-Innovationsmanagement entwickelt die IT kontinuierlich weiter und wird mit Blick auf die IT-Geschäftsausrichtung (engl. business-alignment) gestaltet.

5.3 Architektur von analytischen Informationssystemen mittels drei Schichten

Der allgemeine Aufbau eines Anwendungssystems bedarf der Auswahl einer passenden Anwendungsarchitektur, insbesondere je komplexer das System wird. Eine Anwendungsarchitektur bzw. Softwarearchitektur beschreibt die Strukturen eines IT-Systems, also alle vorhandenen Bausteine, deren Eigenschaften und Beziehungen zueinander, ähnlich einer Gebäudearchitektur [Abts and Mülder(2013), vgl. S. 135ff]. Die Architektur integrierter Informationssysteme (kurz ARIS) ist beispielsweise ein gängiges Architekturmodell von Scheer [Schwarzer and Krcmar(2014), vgl. S. 46-49]. Die technologisch im Aufwind befindlichen Cloud-Lösungen wurden demnach hier nicht behandelt.

Die Drei-Schicht-Architektur als eine weitere mögliche Architektur nach [Abts and Mülder(2013), vgl. S. 268ff] wird, wie in Abbildung 5.7 gezeigt, oft in Informationssystemen angewendet. Sie ist weit verbreitet und hat folgende Schichten [Abts and Mülder(2013), vgl. S. 136-137] und [Schwarzer and Krcmar(2014), vgl. S. 46-49]:

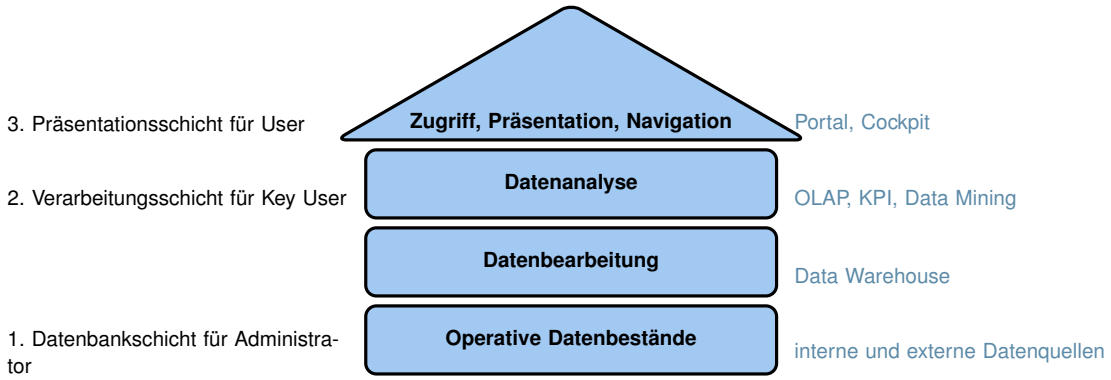


Abbildung 5.7: Aufbau eines Anwendungssystems mittels Drei-Schicht-Architektur [Abts and Mülder(2013), vgl. S. 268ff]

- Die Präsentations Schicht (auch externe Ebene) soll Daten benutzergerecht darstellen und den Dialog zwischen Benutzer und System ermöglichen. Sie ist unabhängig von der gewählten Datenbankstruktur.
- Die Verarbeitungs Schicht (auch logische Ebene) enthält die Anwendungslogik die aus den Eingaben des Benutzers passende Befehlsketten ausführt und dadurch gewünschte Ergebnisse erhält. Sie ist abhängig von der gewählten Datenbankstruktur.
- Die Datenhaltungs Schicht (auch recheninterne Ebene) verwaltet die Daten in einer spezifisch gewählten Datenbankstruktur.

Die Kommunikation zwischen diesen 3 Schichten ist streng geregelt. Jede Schicht bietet der darüber liegenden ihre Dienste an und verwendet wiederum jene Dienste der darunter liegenden Schicht.

Die Vorteile dieser Architektur sind, nach [Abts and Mülder(2013), vgl. S. 136], dass die Schichten weitestgehend unabhängig voneinander und nur von deren Schnittstellen abhängig sind. Daher ist die Abhängigkeit der physischen und programmierten Systemkomponenten minimal und Flexibilität maximal. Durch Spiegelung des Systems können einzelne Schichten im Zuge der Wartung, Adaption, Tests oder Neuentwicklung im laufenden Betrieb verändert werden!

Das 3 Schichten Modell wird durch eine client-server-Anwendung umgesetzt. Das bedeutet, dass nicht mehr alle Schichten auf dem eigenen Computer installiert sein müssen, sondern alle oder einzelne Schichten auf einer Serverfarm laufen. Die Ergebnisse oder Eingaben der einzelnen Schichten werden dann zwischen Serverfarm und Computer mittels Schnittstellen über Netzwerk oder Internet kommuniziert [Abts and Mülder(2013), vgl. S. 138-139].

Informationssysteme sind eine spezielle Art von Anwendungssystemen und folgen als solche den gleichen Prinzipien des Entwicklungsprozesses und Softwarearchitektur.

Analytische Informationssysteme im heutigen Wissensstand nach Abbildung 5.2 folgen hohen Ansprüchen [Abts and Mülder(2013), vgl. S. 265ff]. Nämlich eine umfassende Versorgung aller Unternehmensebenen mit Informationen die der Informationslogistik nach Abschnitt 5.1 gerecht werden. Das schließt unter anderem mit ein, dass Daten sowohl aggregiert als Kennzahlen als auch unbearbeitet überall leicht verfügbar sind. Weiter soll das Informationssystem sowohl permanent die Effizienz der Unternehmensführung steigern und sich in Richtung automatisierter Datenverarbeitung entwickeln.

Die folgenden Kapitel behandeln alle drei Schichten im Detail und behalten dabei den Fokus auf die prototypische Gestaltung für ein mittelständisches Unternehmen wie in Kapitel 6 benötigt.

5.4 1. Schicht: Datenbankschicht

Informationen bzw. Daten sind notwendiger Bestandteil eines Informationssystems. Dabei müssen einige Begriffe kurz geklärt werden, siehe [Abts and Mülder(2013), vgl. S.155-159]:

- “Datenelemente sind die kleinsten logischen Dateneinheiten, die aus einem oder mehreren Zeichen bestehen”
- Ein Datensatz besteht aus mehreren zusammengesetzten Datenelementen, etwa aus den drei Datenelementen: Kundennummer, Name und Vorname.
- “Eine Datei ist eine Zusammenfassung von Daten zu einer sachbezogenen Einheit von in der Regel mehreren Datensätzen. Sie wird unter einem eindeutigen Namen vom Betriebssystem eines Rechners verwaltet.” Sie wird auf physischen Speichermedien gespeichert und vom Betriebssystem verwaltet.
- Formatierte Daten heißen Datensätze, die innerhalb einer Datei immer der gleichen Struktur folgen. Zum Beispiel hätte ein formatierter Datensatz dann immer max. 80 Zeichen, bei dem die ersten 10 Zeichen die Kundennummer sind, die nächsten 35 Zeichen jeweils Name und Vorname.
- “Eine Datenbank ist eine Sammlung von strukturierten, inhaltlich zusammengehörigen Daten. Sie umfasst insbesondere die eigentlichen Nutzdaten.”
- “Ein Datenbanksystem besteht aus einer oder mehreren Datenbanken und einem Datenbankmanagementsystem.”
- “Das Datenbankmanagementsystem (DBMS) besteht aus den Programmen zum Aufbau, zur Kontrolle und zur Änderung und Abfrage der Datenbank.” Führende Hersteller sind z.B. Oracles “Database”, IBMs “DB2”, Microsofts “SQL Server” bzw. “Access” und open-source “MySQL”.
- DBMS haben ebenfalls einen Schichtaufbau “Drei-Ebenen-Architektur”, diese unterscheiden sich durch verschiedene Betrachtungen:

  - Die externe Ebene als Darstellungsform bzw. -ansicht (Sicht, engl. view) zeigt den Nutzern die gespeicherten Daten der Datenbank. Die Sichten zeigen dabei immer nur einen mittels Einschränkungsbefehlen gewählten Teil der Gesamtdaten. Z.B. nur alle Kundendaten einer Region.
  - Die Konzeptionelle Ebene beschreibt sämtliche Daten inklusive logischer Zusammenhänge mittels Datenmodell, etwa dem in Abschnitt 5.4 verwendeten entitiy-relation-model. Zusätzlich regelt sie Zugriffsrechte.
  - Die Interne Ebene regelt die physische Organisation aller Daten, also deren Speicherung und Zugriff.

Datenmodellierung

Das relationale Datenbanksystem (auch Relationenmodell) nach E.F. Codd ist das zur Zeit wichtigste und am weitesten verbreitete Datenmodell und basiert auf dem entity-relationship-model (kurz ER-Modell). Datenbanken, die darauf basieren heißen relationale Datenbanksysteme [Abts and Mülder(2013), vgl. S.165].

Grundlagen des Relationenmodells sind durch das ER-Modell wie folgend geschaffen [Abts and Mülder(2013), vgl. S.160-161]:

- "**Objekte** (synonym: Entitäten) sind einzelne Exemplare von Dingen, Personen oder Begriffen der realen Welt oder der Vorstellungswelt (z.B. der Kunde Meier oder der Artikel mit Artikelnummer 4711). Gleichartige Objekte werden unter dem Begriff Objekttyp (synonym: Entitätstyp) zusammengefasst (z.B. Objekttyp Kunde, Objekttyp Artikel)."

- " Jedes Objekt besitzt verschiedene **Attribute** (Eigenschaften). Beispiel: Name, Straße, PLZ, Ort, Telefonnummer eines Kunden. Ein Objekt besitzt für jedes Attribut einen Wert. Alle Objekte eines Objekttyps besitzen die gleichen Attribute, haben aber in der Regel unterschiedliche Attributwerte."

- "Zwischen Objekten können **Beziehungen** bestehen. Beispiel: Der Kunde Meier bestellt die Artikel 4711 und 5020; der Kunde Schmitz bestellt die Artikel 5020 und 7700."

- "Gleichartige Beziehungen werden als **Beziehungstyp** zwischen den Objekttypen klassifiziert z.B. Kunde "bestellt" Artikel". Die Beziehungstypen werden zum besseren Verständnis als Verben zwischen den Kardinalitäten geschrieben.

- "Nach der Anzahl der an einer Beziehung beteiligten Objekte (**Kardinalität**) unterscheidet man zwischen Eins-zu-Eins, Eins-zu-Viele und Viele-zu-Viele-Beziehungen (1:1-, 1:n- und m:n-Beziehung).

  - Bei einer 1:1-Beziehung ist jedem Objekt des ersten Objekttyps genau ein Objekt des zweiten Objekttyps zugeordnet und umgekehrt. Beispiel: Jeder Student hat genau einen Studentenausweis und jeder Studentenausweis ist für genau einen Studenten ausgestellt.

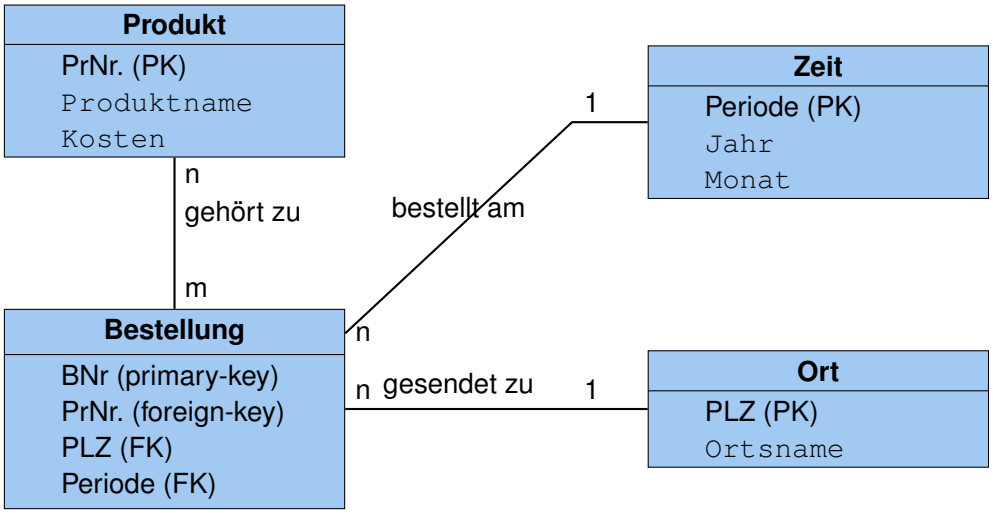


Abbildung 5.8: Beispielhaftes ER-Modell nach [Abts and Mülder(2013), vgl. Abb. 6.6]

  - Bei einer 1:n-Beziehung sind jedem Objekt des ersten Objekttyps keines, eines oder mehrere Objekte des zweiten Objekttyps zugeordnet, jedem Objekt des zweiten Objekttyps ist genau ein Objekt des ersten Objekttyps zugeordnet. Beispiel: Ein Professor betreut mehrere Studenten.
  - Bei einer m:n-Beziehung sind jedem Objekt des ersten Objekttyps keines, eines oder mehrere Objekte des zweiten Objekttyps zugeordnet und umgekehrt. Beispiel: Ein Kunde hat mehrere Artikel bestellt, ein Artikel wurde von mehreren Kunden bestellt."

- "Objekttypen werden durch Rechtecke, Beziehungstypen durch Kanten, die Rechtecke verbinden, dargestellt. An den Enden einer Kante wird die Kardinalität des Beziehungstyps eingetragen. Oft ist zusätzlich die Bedeutung der Beziehung notiert."

ER-Modelle zeigen die verwendeten Daten in Datenbank-Klassen unterteilt, listen die mitgeführten Attribute auf und geben Aufschluss über die gegenseitige Relation [Abts and Mülder(2013), vgl. S.160-167], siehe Abbildung 5.8.

Das Relationenmodell wie etwa in Abbildung 5.9 gezeigt, überträgt das ER-Modell in ein datenbankgerechtes Modell [Abts and Mülder(2013), vgl. S.165ff]. Alternativ können sogenannte "Star" bzw. "Snowflake " Schemata zur Erstellung eines Relationenmodells verwendet werden [Frick et al.(2009)Frick, Servaes, Abts, Mehrtens, Söhnchen, Mülder, Stegemerten, and Westheide, vgl. S.97-98]. Prinzipieller Aufbau eines Relationenmodells:

- Jedes ER-Modell kann in ein Relationenmodell überführt werden [Frick et al.(2009)Frick, Servaes, Abts, Mehrtens, Söhnchen, Mülder, Stegemerten, and Westheide, vgl. S.606].
- Dafür werden **Relationen** (dies wäre ein Objekttyp im ER-Modell) benötigt, die man sich als zweidimensionale Tabellenblätter mit fixer Spaltenanzahl und beliebiger Zei-

lenanzahl vorstellen kann. Diese Tabellen sind nichts anderes als Datenbanken, wobei verglichen mit dem ER-Modell jede Zeile einem Objekt und jede Spalte einem Attribut entspricht.

- Jede Relation wird mit einem oder mehreren **Schlüsseln** verbunden, siehe Abbildung 5.9. Schlüssel sind eindeutige Zahlen oder Namen oder Zeichenketten mit denen man ähnlich einer Postadresse verschiedene Datenbanken miteinander verbinden kann. Dafür können eigene Tabellenblätter sogenannte **Koppeltabellen** genutzt werden, um mittels mehrerer Schlüssel eine m:n-Beziehung aufzubauen. Spalten mit einem Schlüssel werden meist unterstrichen um sie von den normalen Attributen zu unterscheiden.

- Durch **Normalisierung** und ihre 3 Regeln (Normalformen), wird die funktionale Unabhängigkeit zwischen den verschiedenen Attributen sichergestellt und somit eindeutige Datenstrukturen [Abts and Mülder(2013), vgl. S.168-170].

Die praktische Umsetzung von Datenmodellen erfolgt in Datenbanken, welche in ihrer einfachsten Form mit Microsoft Access oder der gängigen SQL Datenbank abgebildet werden können [Abts and Mülder(2013), vgl. S.157].

Alternativ zum Relationenmodell kann ein Klassenmodell genutzt werden, in der objektorientierten Modellierung (mit unified-modeling-language, kurz UML) fasst dies die Inhalte eines Daten- und Funktionsmodells zusammen und erstellt so einen technischen-sozialen Entwurf [Gumm and Sommer(2013), vgl. S.840].

Vor der Eigenerstellung eines neuen Datenmodells ist zu empfehlen, Datenbankanbieter zu kontaktieren. Die meisten Geschäftsprozesse sind bereits tausendfach in Datenbanken modelliert worden und als best-practice extern erhältlich.

Datensammlung

Die Organisation und Beschaffung der richtigen Daten werden in den folgenden Kapiteln erläutert.

Bereits bei der Datensammlung, also der Erschließung von Datenquellen und der Einpflege in Datenbankstrukturen, muss entschieden werden, welche Organisationsform, Zeit oder Messgröße als Stammdaten benötigt werden. Bei den Bewegungsdaten kann anhand der Aussagekraft, Verfügbarkeit und Messbarkeit erst entschieden werden, welche möglich sind.

Bei der Datensammlung können je nach Datenquellen strukturierte wie unstrukturierte Daten aus internen und externen Quellen entnommen werden, [Krcmar(2015), vgl S. 183-187]. Beispiele sind [5]:

- Externe Quellen sind open-government oder private Finanzdienstleister für strukturierte Daten. Diese können direkt aus dem Internet als interne strukturierte Daten eingepflegt werden.

[5] vgl. `https://en.wikipedia.org/wiki/Information_management` (11.8.2015)

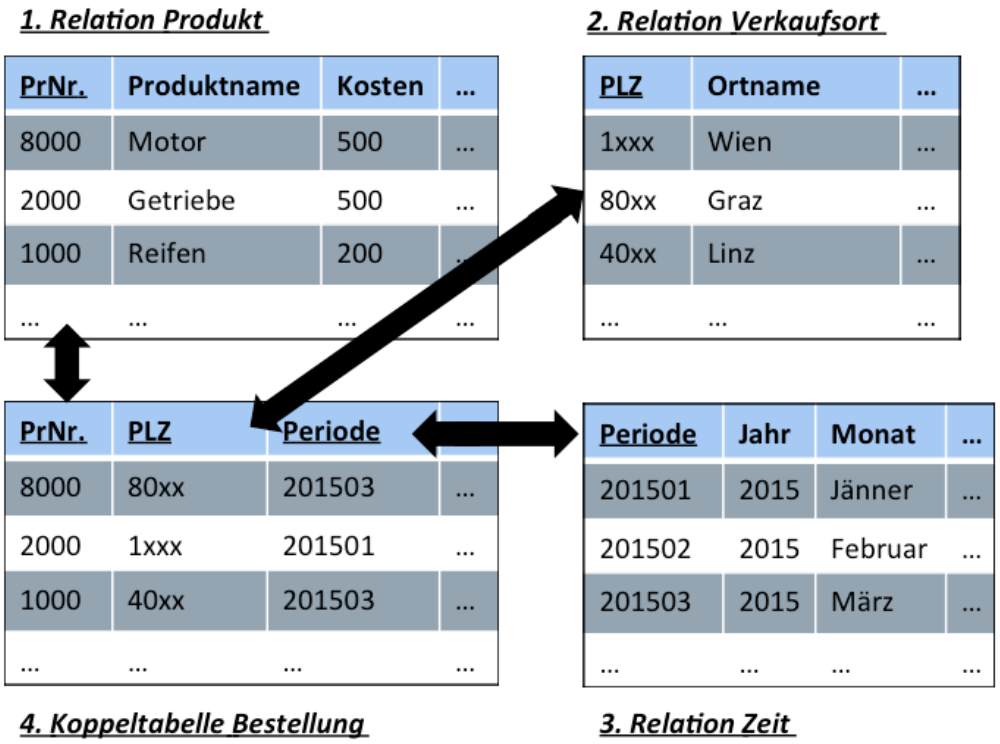


Abbildung 5.9: Beispielhaftes Relationenmodell [Schwarzer and Krcmar(2014), vgl. Abb. 2-11]

- Unstrukturierte externe Daten sind z.B. Zeitungen oder social-media.
- Interne Quellen sind Protokolle für unstrukturierte Daten und operative Datenbanken für strukturierte Daten.

Zu denken gibt dabei das Gesetz von Finagle [6], das besagt: Die Information die du hast, ist nicht welche du willst, die Information die du willst, ist nicht die, die du brauchst, die Information die du brauchst, ist nicht jene die du erlangen kannst und die Information die du erlangen kannst, kostet mehr als du bereit bist zu zahlen [Frick et al.(2009)Frick, Servaes, Abts, Mehrtens, Söhnchen, Mülder, Stegemerten, and Westheide, vgl. S.61].

Klassische Datenbanksysteme wie in Abschnitt 6.2 geschildert, verwenden strukturierte Daten. [Krcmar(2015), S. 44]. Generell werden Datentypen nach folgenden Kriterien unterschieden [Gerhard(2014), F.89]:

- strukturierte Daten, wobei deren Organisation über strukturgebende Informationen sogenannten Metadaten passiert. Mittels Metadaten werden andere Daten beschrieben

[6] vgl. `https://de.wikipedia.org/wiki/Finagles_Gesetz` (11.8.2015).

und strukturiert. Sie können Datenformate, Datentypen, erlaubte Eingabewerte oder semantische Bedeutung (Erklärungen der Daten) beinhalten.

- semistrukturierte Daten, können teilweise strukturiert sein, dies ist aber nicht durchgängig und eindeutig.
- unstrukturierte Daten, weisen auf den ersten Blick keine Struktur auf, z.B. Bilder oder Emails

Die strukturierten Daten lassen sich vielfach weiter unterteilen, im Risikomanagement geschieht das nach Art der Messbarkeit. Qualitative Daten können Interviews, Meinungen oder visualisierte Informationen sein und quantitative Daten haben konkrete Zahlenwerte. Die Messungen dieser Daten erfolgt als [Biffl(2010), F. 26]:

- Direkte Messung, also ein direktes zählen des messbaren Objekts, z.B. einer Stückzahl oder Laufzeit.
- Indirekte Messung, bedarf eines Zwischenschrittes wie die Berechnung anhand von Algorithmen und Naturgesetzen.
- Objektive Messung, wobei Ergebnis und Entscheidungsbereiche Zahlen als Kriterium haben.
- Subjektive Messung, welche die Einschätzung eines Teams oder ExpertIn widerspiegeln.

Stammdaten und Bewegungsdaten

Die Entscheidung ob es sich um Stammdaten oder Bewegungsdaten handelt, muss bei jedem Datensatz während der Modellierung des Datenmodells in Form von Datenbanken getroffen werden.

- Stammdaten sind Daten die unternehmensweit von verschiedensten Abteilungen und IT-Systemen verwendet werden, z.B. Kunden- oder Materialstammdaten [Krcmar(2015), S. 43]. Sie sollen trotz heterogener Verwendung eine Qualität und Redundanzfreiheit sicherstellen. Stammdaten werden in Datenbanken nicht mit allen Dimensionen verknüpft, da sie nicht auf Perioden oder Abteilungen aufgeteilt werden müssen, dies reduziert beim Datenwürfel die Ebenenanzahl und erhöht somit die Rechengeschwindigkeit.
- Bewegungsdaten werden im laufenden Betrieb ständig geändert, so z.B. Finanz-Kontensalden- oder Produktionszahlen. Die Datenbanken müssen auf Versionierungen, Benutzerzugriff, etc. eingestellt sein und eine Änderungshistorie gewährleisten. In den Datenbanken sind sie meist mit allen Dimensionen verknüpft, da sie auf Perioden oder Abteilungen aufgeteilt werden müssen!
- Die in Abschnitt 5.4 beschriebenen Metadaten sind von Stammdaten zu unterscheiden. Metadaten werden im Datenbankmanagement zur Strukturierung verwendet und Stammdaten sind bereichsübergreifende, geschäftliche Unternehmensdaten.

5.5 2. Schicht: Verarbeitungsschicht für Datenanalyse und -bearbeitung

Die reine Extraktion von Daten aus der 1. Schicht (Datenhaltung) in Form der simplen Ausgabe in der 3. Schicht (Präsentation) ist trivial. Erst eine Transformation der Daten innerhalb der 2. Schicht (Verarbeitungs- bzw. Logikschicht) in Form von Verdichtung (Die Summierung von Daten verschiedener Ebenen, z.B. Jahresumsatz), Anreicherung (die Berechnung von Kennzahlen, z.B. Gewinn) oder Datenanalyse (z.B. mittels OLAP Datenwürfel, siehe Abschnitt 5.5) schafft den entscheidenden Mehrwert eines analytischen Informationssystems [Abts and Mülder(2013), vgl. S.272-282].

Die Verarbeitungsschicht ist auch die Ebene auf der Simulationsabläufe oder Verformelung für komplexe Berechnungen definiert und die dazugehörigen Variablen mit den passenden Datenbanken verknüpft werden. Somit ist diese Ebene nicht mehr unabhängig von der Datenbankwahl.

Datenanalyse mittels OLAP

OLAP (Abkürzung für online-analytical-processing) ist eine Datenbankmodellierung speziell für analytische Systeme, die eine Ermittlung mehrdimensionaler Kennzahlen zum Zwecke der Analyse ermöglicht, nach [Abts and Mülder(2013), vgl. S.279-282]. Dadurch unterscheidet sich das analytische OLAP prinzipiell von dem operativen Datenverarbeitungsprinzipien (transaktionsorientierten Datenverarbeitungen kurz OLTP). Nach Abschnitt 5.4 ist das OLTP auf anlegen, ändern oder suchen von Datensätzen spezialisiert, im Zuge eines z.B. typischen ERP Systems. Die Idee und 12 Anforderungen an OLAP Systeme stammen von E.F. Codd, dem Erfinder der relationalen Datenbanken, darauf wird hier nicht näher eingegangen. OLAP und OLTP unterscheiden sich etwa bei der Datenstruktur (OLAP multidimensionale Tabellen und OLTP flache Tabellen), Datenmanipulation (bearbeiten einzelner Datensätze vs. Analyse großer aggregierter Datenmengen), Datenquelle (OLAP intern und extern und OLTP nur intern), etc. [Frick et al.(2009)Frick, Servaes, Abts, Mehrtens, Söhnchen, Mülder, Stegemerten, and Westheide, vgl. S.87-90].

Das mehrdimensionale Datenschema eines OLAP kann mittels “multidimensionalen Datenbanksystem” oder dem in dieser Arbeit bevorzugten relationalen Datenbanksystem (siehe Abschnitt 5.4) realisiert werden [Frick et al.(2009)Frick, Servaes, Abts, Mehrtens, Söhnchen, Mülder, Stegemerten, and Westheide, vgl. S.95-98].

Die Mehrdimensionalität wird in Abbildung 5.10 durch einen Datenwürfel grafisch erklärt. Diese Mehrdimensionalität erlaubt unterschiedliche Sichtweisen der mittels relationalen Datenmodell verknüpften Dimensionen, wie in Abbildung 5.11 gezeigt. Dabei beschränkt sich die Mehrdimensionalität nicht etwa, wie im gezeigten Beispiel auf drei Dimensionen, sondern kann auf Kosten einer erhöhten Rechenzeit beliebig hohe weitere Dimensionen haben.

Business Intelligence

“We are drowning in information and starving for knowledge.” [Naisbitt, 1982]

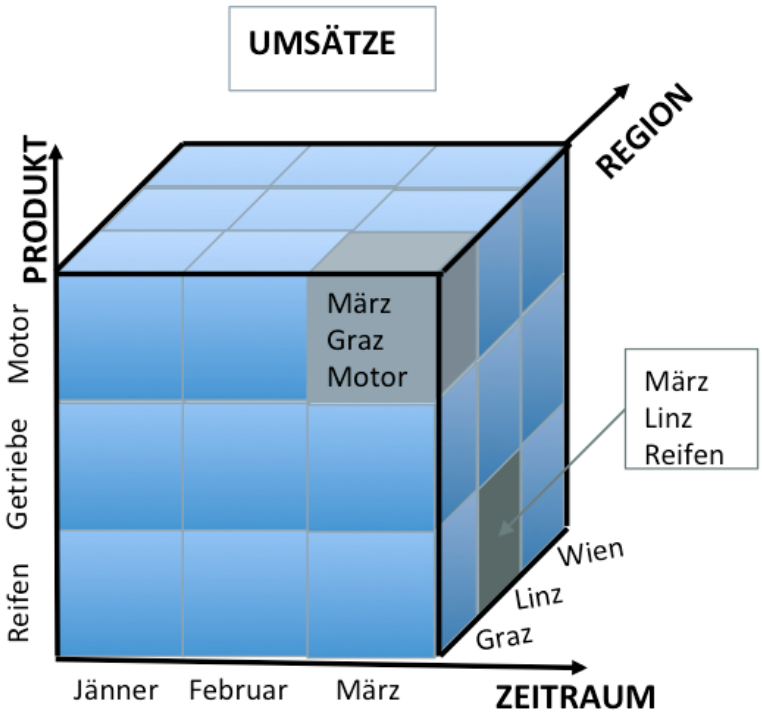


Abbildung 5.10: Mehrdimensionaler OLAP-Datenwürfel [Abts and Mülder(2013), vgl. Abb. 9-10]

Moderne Unternehmen haben Zugriff auf eine große Menge an Daten. Wie in Abbildung 5.2 geschildert, entwickeln sich die analytischen Informationssysteme in Richtung big-data und Industrieunternehmen erhalten durch ihre z.B. operative enterprise-ressource-planning-Systeme viele hochstrukturierte Daten. Doch für strategische Entscheidungen und Berichterstattung braucht es oft passende business-intelligence Software mit künstlicher Intelligenz um daraus anwendbare Informationen zu erhalten. Analysen werden in drei Arten eingeteilt. Erstens in die Beschreibenden (engl. descriptive) indem sie relevante Informationen zu Fragestellungen filtern. Zweitens die Vorhersagenden (engl. predictive), sie finden Zusammenhänge und Verknüpfungen in den Daten der Fragestellung. Drittens in die vorgeschriebenen Analysen (engl. prescriptive), sie berechnen den besten Lösungsweg und geben Empfehlungen ab [7].

Als Überblick dient der von Gartner erstellte Benchmark in Abbildung 5.12 [8].

[7] vgl. https://de.wikipedia.org/wiki/Business_Intelligence#Business_Analytics (3.8.2015).

[8] vgl. https://www.gartner.com/doc/2989518/magic-quadrant-business-intelligence-analytics (1.8.2015).

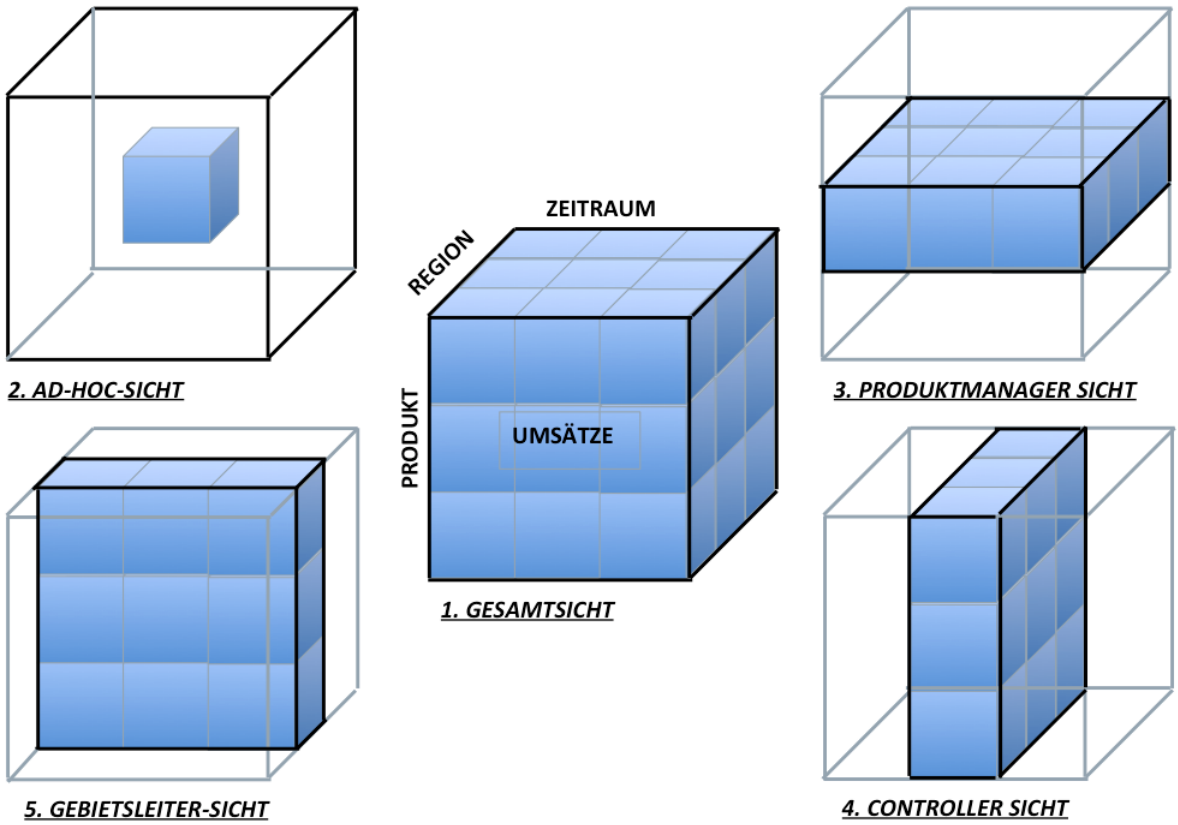


Abbildung 5.11: Navigation und Datenanalyse mit OLAP-Datenwürfel [Abts and Mülder(2013), vgl. Abb. 9-11]

So werden laut Gartner Marktführer wie SAP BO, Qlik, Tableau, SAS oder Mico-Strategy nach 13 kritischen Fähigkeiten bewertet [9]. Dabei sind 1 bis 6 als Befähigungen (enable) zusammengefasst, weiters 7 bis 10 als Produktionsfähigkeiten (produce) und 11 bis 13 als Konsumationsfähigkeiten (consume):

1. Ermöglicht ein data-mashup and modelling dem Nutzer Daten aus Datenbanken einfach per z.B. drag-and-drop zu kombinieren, sortieren oder analysieren. Siehe Abschnitt 5.4

2. Interne Integrationsmöglichkeiten der Plattform mit anderen Systemen im Unternehmen.

3. Plattform Administration, Nutzer Administration, Rechte, Rollen, Skalierbarkeit und die 3 klassischen Sicherheitskriterien Vertraulichkeit, Integrität, Verfügbarkeit nach Abschnitt 5.2

[9] vgl. `http://www.gartner.com/technology/reprints.do?id=1-2ADAAYM&ct=150223&st=sb` (3.8.2015).

4. data-metadaten-management, siehe Abschnitt 5.4 um von einer zentralisierten Administration unternehmensübergreifende Dokumentvorlagen oder Datenbank Dimensionen wie Zeit, Organisationseinheiten, Rechte, KPIs, etc. zu verwalten.
5. Nutzung von Cloud Plattformen und Services.
6. Individuell anpassbare Plattform um einerseits Dashboards, Reports und Analysen selbst adaptieren und gestalten und BI Komponenten in andere Anwendungssoftware wie z.B. Business Prozesse integrieren zu können.
7. Interactive Experten Datendarstellung, -suche und -analyse mittels free-form-interaktive-exploration.
8. Interaktive Dashboards welche Analyse und Daten auch für authorisierte Dritte bereitstellt.
9. Automatisierte IT-Reports und Dashboards, welche zudem noch parametisiert, benutzerfreundlich und stylisch sind.
10. Traditionellere Datenstrukturen, welche Datenanalysen der Benutzer mittels z.B. OLAP ermöglichen, ohne das die IT-Spezialisten kontaktiert werden müssen.
11. Mobiltelefon Apps dienen als publizierendes und interaktives Ein- und Ausgabegerät.
12. Integrierter Chat oder soziales Netzwerk zum Diskurs der Benutzer
13. Besteht für IT-Entwickler ein Software Development Kit mit bestenfalls offenen Entwicklungsstandards (open source). Dies ermöglicht jedem Plattformnutzer individuelle Anpassung, Einbindung und Erweiterungen.

Der ganze Bereich ist Gegenstand schneller Entwicklungen und nicht Bestandteil dieser Arbeit.

5.6 3. Schicht: Präsentationsschicht für Nutzer

Zwischen Informationssystem und Benutzer braucht es Benutzerschnittstellen (engl. user-interface) die eine Visualisierung von Informationen, Navigationsmöglichkeiten und Eingabemöglichkeiten gleichermaßen ermöglichen [Abts and Mülder(2013), vgl. Kp.9.6].

Das user-interface ist verantwortlich für die sogenannte user-experience und allgemeiner noch für die Usability (Benutzerfreundlichkeit, Ergonomie) welche nach ISO 9241 genormt ist [10].

Die human-computer-interaction bzw. media-informatics, wird wie in Abschnitt 5.2 ersichtlich, nicht immer als eigenständige Disziplin innerhalb der Informatik oder gar als dem Design zugehörig betrachtet [Purgathofer(2006), vgl. S.1]. Purgathofer sieht seit Beginn der

[10] `https://en.wikipedia.org/wiki/User_interface_design` (24.07.2015)

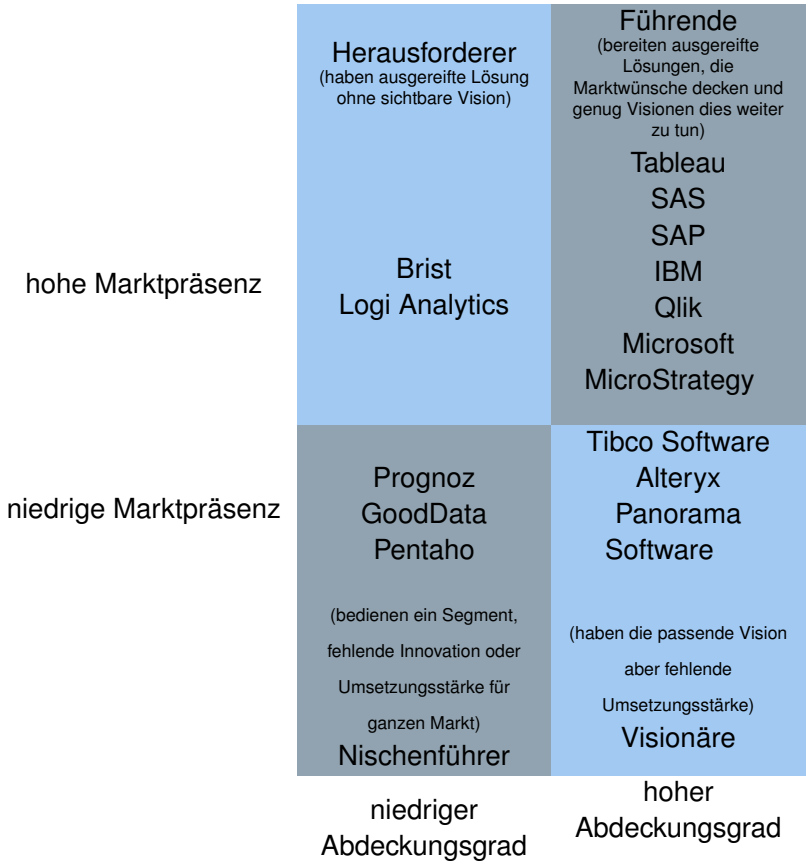


Abbildung 5.12: Gartner Magic Quadrant für “Business Intelligence and Analytics Plattformen”, [Gartner(2011), vgl. S.7ff]

Informatik, im Zuge der Softwarekrise 1968, das software-design als zu Unrecht vernachlässigte Sparte im Zuge des ingenieursmäßigen Aufbau von Software. Falsche Designkonzepte seien ein nicht unwesentlicher Grund für schlechte Software. Dementsprechend muss das Design am Anfang des Produktlebenszyklus erstellt werden, erst im Anschluss alle folgenden Phasen der Entwicklung, Marketing und Management beginnen und sich danach richten [Purgathofer(2006), vgl. Kp. 8]!

Nach Purgathofer gibt es 6 Faktoren, die für eine qualitative Medienerfahrung zu beachten sind [11]. Sie sind auch im Zuge der Gestaltung der Präsentationsschicht sinnvoll:

1. Die Benutzergruppe (engl. communities) muss immer in Betracht gezogen werden, eine Zusammenarbeit ist sinnvoll.

[11] vgl. `http://www.slideshare.net/peterpur/6-factors-to-consider-in-quality-of-media-experience` (11.8.2015).

2. Placebo-Effekte wie Hochglanzgrafiken oder technische Spielereien sollen nicht Funktionalität vortäuschen. Es sollen immer die Kernfunktionen auch die Aufmerksamkeit der Nutzer und Entwickler erhalten.

3. Authentizität (engl. authenticity) des gesamten Systems, bezüglich Fakten (und keiner fiktiven Scheingenauigkeit), Objektivität, Relevanz und Vollständigkeit.

4. Interaktion ist die Schnittmenge von Benutzerfreundlichkeit (engl. usability), Nützlichkeit (engl. utility) und Beliebtheit (engl. likeability). Dabei soll eine Benutzeroberfläche benutzbar (engl. usable), nutzbar (engl. useful), begehrt (engl. desirable), zugänglich (engl. accessible), vertrauenswürdig (engl. credible) und auffindbar (engl. findable) sein. Das Designprinzip simplicity von Apple ist dabei ein gutes Veranschaulichungsbeispiel, weniger ist mehr!

5. Im Speziellen kann auch eine Ästhetik bei der Bedienung (engl. interaction-aesthetics) festgestellt werden. Diese wird erreicht durch Anpassungsfähigkeit (engl. pliability), Rhytmus (engl. rhythm), Dramatik (engl. dramaturgical-structure), Übergangsfreiheit (engl. fluency), Kontrolle (engl. control), etc. Allgemein folgt gute Ästhetik (engl. aesthetics) folgenden 4 Prinzipien nach [Schifferstein and Hekkert(2011), vgl. S. 165-166].

    - Maximaler Effekt mit minimalen Mitteln (engl. maximum-effect-for-minimum-means).
    - Einheitlich trotz Vielfalt (engl. unity-in-variety). Das bedeutet, dass soviel Vielfalt oder Komplexität wie möglich, mit einer maximalen Einheitlichkeit oder Ordnung dargestellt werden soll.
    - Das Fortschrittlichste aber noch akzeptierte nehmen (MAYA-Prinzip, engl. most-advanced-yet-acceptable).
    - Optimale Verbindung (engl. optimal-match) zwischen gewünschten Funktionen, Benutzererfahrung und Organisation finden.

6. Teile (engl. sharing) Erfahrungen und Designs. Copyright Gesetze gehören beachtet.

Die folgenden grafischen Elemente und Designmethoden finden sich in den meisten Informationssystemen in Abschnitt 5.1 wieder:

- Gängige Elemente der Navigation sind Workflows oder Reiter die als Leisten alle möglichen Bereiche verknüpfen.

- Gängige grafische Benutzerschnittstellen (engl. GUI) sind Hyperlinks, aufklappbare Details, Diagramme, Tabellen, Ampel, Tachometer, Landkarten etc. sie eigenen sich sowohl zur Eingabe als auch Darstellung von Informationen.

- Dashboards bzw. management-cockpits sind gängige Formen von übersichtlichen Informationsvermittlung.

KAPITEL 6

Bericht einer Risikomanagement Informationssystem Entwicklung

Dieses Kapitel setzt die im Kapitel 5 erarbeiteten Grundlagen von Informationssystemen praktisch um.

Generell unterstützt das folgende Risikomanagement Informationssysteme, die im Risikomanagement tätigen Personen bei der Erfüllung ihrer täglichen Aufgaben, insbesondere die Risikoverantwortlichen als Nutzer und den zentralen Risikomanager als Administrator. Zudem soll hier ausdrücklich darauf hingewiesen werden, dass die Gestaltung auf die hauseigenen Anforderungen und Bedürfnisse der Nutzer konzentriert sein soll.

Das Verständnis liegt hier vorwiegend auf der Annahme, dass sich die Mitarbeiter und Führungskräfte als Nutzer des Risikomanagementsystems nur oberflächlich mit IT-Lösungen befassen müssen und die Bedienung dadurch intuitiv erfolgen muss. Die Bedienung wird als Workflow (Flussdiagramm) mit einblendbaren Erklärungen umgesetzt.

Die Vorteile eines Informationssystems zeigen sich vor allem durch die gegebene Übersicht, automatische Versionierung, Historie, Zugriffskontrolle, Automatisierung und Zentralisierung der Datenquellen. Diese aufgelisteten Punkte zeigen die zwingende Notwendigkeit einer IT-Lösung, aber auch, dass es kurz gesagt, die gleichen Vor- und Nachteile eines jeden Informationssystems sind.

Der Aufbau des Projekts und dieses Kapitels richtet sich anhand der Phasen des in Abbildung 5.6 geschilderten Software Entwicklungsprozesses. Da das Projektziel ein prototypisches Anwendungssystem für die Erforschung der Risikoprozesse und Kundenanforderungen war, orientierte sich der Entwicklungsprozess ebenfalls an der Prototyping Methode. Die Kundenanforderungen wurden in Zusammenarbeit und für die vorhergesehene Nutzung bei der mittelständischen Ottakringer Getränke AG ausgelegt.

Der entwickelte Prototyp zu dieser Arbeit zielte auf ein computerunterstütztes Informationssystem mittels 3-Schichten Architektur hin und wurde im prevero p7 maple leaf umgesetzt. Details wie eine Übersicht über die Funktionen und Einstellungsmöglichkeiten werden im folgenden Kapitel geschildert.

6.1 Analysephase zur Ermittlung der Anforderungen

Die Aufgabe einer jeden Analyse in der Software Entwicklung ist die Entdeckung der Systemanforderungen und die daraus folgende Entwicklung eines passenden Lösungsmodells. Dabei müssen die Analysemethoden sowohl die betriebswirtschaftlichen Anforderungen an eine Softwarelösung für Unternehmen [Denk(2008), S.157-158] abdecken als auch die Anforderungen eines Informationssystems [Krcmar(2015), S.67]. Diese Phase wird auch oft als requirement-engineering bezeichnet und beantwortet folgende Fragen:

- Warum soll ein System entwickelt werden?
- Welche Funktionen soll das System haben?
- Welche Leistungen (engl. performance), in Form von z.B. Nutzerzahl oder Schnelligkeit, soll das System haben?
- Welche Einschränkungen (engl. constraints) sollen respektiert werden?
- Wie kann die Funktionstüchtigkeit getestet werden?

Die Einteilungen in der nachfolgenden Tabelle 6.1 erfolgen nach der, in Abschnitt 5.3 erwähnten, drei Informationssystem-Schichten Datenbank (DB), Businesslogik (engl. business-intelligence (BL) und Benutzeroberfläche (engl. user-interface (BO). Erweitert durch eine vierte Gruppe, die die allgemeinen Anforderungen eines Risikomanagementsystems an die Organisation (OR) widerspiegelt. Die hier beschriebenen Anforderungen sind zur Umsetzung eines softwareunterstützten Risikomanagement Informationssystems notwendig [Neuhauser(2011), vgl. Kp.6]. Die Anforderungen können mit steigendem Reifegrad oder nach unternehmensspezifischen Gegebenheiten angepasst und erweitert werden. Ziel ist es das Risikomanagementsystem bestmöglich an die individuellen Bedürfnisse der Nutzer anzupassen.

Ziel	Beschreibung	Ergebnis	IT Umsetzung
OR-1	Ziele und Strategien sind auf jeder Unternehmensebene definiert.	Strukturierte und dokumentierte Ziele.	Dimension Ziele.
OR-2	Eine Risikostrategie ist formuliert und alle Prozesse richten sich am angestrebten Risikoappetit.	Risikomanagement Handbuch.	Online Zugriff.

OR-3	Die gelebte Risikokultur unterstützt eine proaktive Auseinandersetzung mit Risiken.	Ton von der Geschäftsführung und Vorgabe der Risikophilosophie.	Zugriff mit eigenem Account für jeden Risikoeigner.
OR-4	Geschäftsprozesse sind vorhanden, haben einen akzeptablen Reifegrad und sind mittels Prozessdokumentation zugreifbar.	Prozess Flowcharts wie etwa Abbildung 4.5 ermöglichen die Verknüpfung der Prozesse mit Risiken.	Dimension Prozess.
DB-1	Die Organisation und deren Aufbau wird mit Hierarchien, Abteilungen, Standorten und Tochterfirmen abgebildet.	Risikokonten Plan nach Abschnitt 4.5	Dimension Einzelperson, Funktion und Hierarchie.
DB-2	Das Unternehmen wird in Risikobereiche unterteilt.	Organigramm mit verantwortlichen Risikoeigner pro Geschäftseinheiten, meist die Abteilungsleitung.	Benutzerverwaltung und Verwaltungsansicht, wie in Abbildung 4.2 gezeigt.
DB-3	Einzelne Risiken werden einer Risikokategorie zugeteilt und erhalten eine, auch für Fremde nachvollziehbare, Bezeichnung.	Risikokategorien als grundlegendes Schema für die Risikonummer, siehe Abbildung 4.8	Dimension Risiko mit abgebildeten Nummernschema.
DB-4	Zuteilung des Risikos zu einer oder mehreren Geschäftseinheiten.	Risikobereiche wurden mit Risikokategorien verknüpft. Über die Risiko-Kontonummern werden Geschäftseinheiten und damit automatisch Risikoeigner, zugeteilt.	Ein individuelles Tabellenblatt bzw. Datenwürfel mit verknüpften Risiken und Hierarchie pro Risikoeigner.
DB-5	Für die Analyse und Beurteilung des Risikos können Daten aus verschiedensten Datenquellen eingebunden werden.	Manuelle oder automatisierte Schnittstellen.	
DB-6	Ein Risiko erhält eine Analyse und die Bedeutung wird berechnet oder geschätzt. Begründungen über Daten und Kennzahlen sind wünschenswert.	Wahlweise qualitative oder quantitative Skalen pro Risiko, inklusive Wertintervallen.	Dimension Skalenart, Metrik, Bedeutung und Häufigkeit

DB-7	Jede Abteilung und jede Risikokategorie kann eigene Skalenbeschriftung verwenden, um deren Höhe und Betitelung den eigenen Anforderungen anzupassen.	Der Risikomanager definiert nur die Skalenart und deren Messgröße.	Verknüpfung Skalenart und Metrik mit Hierarchie.
DB-8	Für die Bewertung haben einzelne Risikokategorien eine definierte Wahrscheinlichkeitsverteilung und/oder Datenbasis.	Abbildung 3.10 als Übersicht der Verteilungen.	Im Standardfall nach Abbildung 3.12 werden Risiken als normalverteilt angenommen, in Spezialfällen können durch Formeleingabe im Arbeitsblatt andere definiert werden.
DB-9	Für jedes Risiko ist eindeutig auszuwählen, welche Identifikations- und Bewertungsmethode mit welchen Parametern auf Basis welcher Daten gewählt würde.	Auswahl Methode VaR, Fragebogen oder Expertenschätzung.	Dimension Methode und Auswahl im Arbeitsblatt. Je nach Methode angepasste Reports.
DB-10	Korrelationen zwischen den Risiken können hinterlegt werden. Dies bedarf einer ausreichenden Datenbasis und ist für fortgeschrittene Aggregationen notwendig.	Aufgrund des heutigen Wissensstands und Datenarmut ist dies nur als Prototyp ohne Werte vorhanden.	Umsetzung als Korrelationsmatrix mit Werteeingabe zwischen 0 bis 1.
DB-11	Im Zuge der Risikosteuerung werden für Risiken Maßnahmen getroffen, diese beinhalten Umsetzungsdetails.	Ein online Maßnahmenplan, wie etwa in Abbildung 4.13, beinhaltet Felder mit Angaben wie Umsetzungszeitraum, Kosten, Verantwortlichkeiten, Komplexität. Das ermöglicht Projektmanagement .	Dimension Maßnahme.
DB-12	Im Zuge der Risikoüberwachung wird für jedes Risiko die Kontrolle, die Berichtsperiode sowie Priorität festgelegt.	Der Kontrollprozess wie etwa interne Kontrolle oder Compliance sind im Projekt eingebunden und haben eigene Dienste.	Eigene Benutzeroberfläche und Workflows für Kontrolle abgebildet. Ein Arbeitsblatt nach Abbildung 4.15 wurde als Kontrollplan gestaltet.

DB-13	Adressaten können für Risiken oder Bereiche festgelegt werden. Es können dann adressatenbezogene Berichte erstellt werden.	Über die Kontonummer sind sowohl Abteilung als auch Tochterfirma definiert. Darüber hinaus können Berichte manuell an Adressaten erstellt werden.	Arbeitsblätter als Reports gestaltet.
DB-14	Der Adressat kann je nach Risikoausmaß und aktueller Situation variieren. Es müssen also Schwellwerte festgelegt werden können.	Weiters können spezielle Risiken wie Lebensmittelsicherheit, Compliance oder Lebensgefährdung speziell markiert werden.	Im Stammblatt wird dies als Toprisiko-Kästchen umgesetzt .
DB-15	Experten können als Verantwortliche den Risikokategorien zugeteilt werden.	Einzelne Auswahlfelder sind für Risikoeigner eingeschränkt oder vordefiniert.	Experten greifen auf die Admin-Arbeitsansicht des Arbeitsblattes, Datenwürfel oder Dimensionselemente zu.
DB-16	Der komplette Risiko Prozess wird versioniert und mittels einer Historie dokumentiert.	Versionierung sowohl manuell pro Änderung als auch automatisiert pro Periode.	Dimension Berichtsperiode und Dimension Änderung.
DB-17	Mittels Status ist die Gültigkeit und Aktualität eines jeden Risikos, Maßnahme oder Arbeitsblattes gewährleistet.	Manuelle Status sind etwa in Arbeit oder ungültig und automatisierte etwa veraltet.	Dimension Status.
DB-18	Im Zuge des Risikoprozesses werden schrittweise weitere Eingaben zur genaueren Beschreibung des Risikos gefordert und so ein detailliertes Verständnis aufgebaut.	Periodisch wiederholender Workflow mit Alarming.	Umsetzung als online Fragebogen nach Abbildung 4.16 und im Arbeitsblatt workflow.
BL-1	Login mittels Benutzer und Kennwörter.	Übersicht wer, was im System veränderte.	Administratoransicht für Verwaltung von Rollen- und Berechtigungsverteilung, siehe Abbildung 4.2

BL-2	Das System muss eine Integration aller Planungsebenen (operativ, taktisch, strategisch) unterstützen. Dies betrifft sowohl horizontale als auch vertikale Teile der Aufbauorganisation.	Das 3-lines-of-defense Modell in Abbildung 3.4 und Abbildung 4.3 unterteilt die Aufgabenfelder. Prinzipiell werden die Schnittstellen primär vom Risikomanager verantwortet, welcher als Bindeglied dieser Ebenen fungiert.	Durch die Zuteilung von Verantwortlichkeiten, gemeinsamer Datenbasis und verschiedenen, dem User entsprechenden, Arbeitsblättern wird dies umgesetzt.
BL-3	Erstellung der für die Geschäftsführung wichtigen Toprisiken.	Risiken werden auf operativer Ebene vom Risikoeigner erfasst und in der Hierarchie nach oben aggregiert. Aggregation ist die Aufgabe des Risikomanagers.	Umsetzung grafisch als Risikomatrix und zusätzlich sortiert als Rangliste.
BL-4	Der Workflow besteht aus den normgerechten Prozessen der Risikoidentifikation und -analyse, Risikobewertung, Risikosteuerung, Risikokommunikation und Risikoüberwachung, siehe Abbildung 2.2 oder Abbildung 3.5.	Arbeitsblatt Prozessübersicht als Startfenster.	
BL-5	Der RM-Rahmen wird in der Risikopolitik beschrieben und top-down von der Unternehmensführung vorgegeben.	Zugriff RM-Handbuch als Link möglich.	
BL-6	Periodische Kontrollen und Verbesserungen im Sinne einer kontinuierlichen Verbesserung finden laut Risikopolitik statt.	Datumseingaben im Maßnahmen- und Kontrollplan erinnern sowohl an periodische als auch antizyklische Überprüfungen	Automatisierung der Erinnerung via Email.
BL-7	Wenn ein Risiko einen definierten Maximalwert überschreitet, muss der Risikomanager und der nächsthöhere Vorgesetzte informiert werden.	Maximalwerte werden in der Risikomatrix in Abbildung 4.9 als rote Bereiche angezeigt.	Benachrichtigung via automatischer Email.

BL-8	Das System unterstützt die Kommunikation und Dokumentation von Risiken und Maßnahmen, die mehrere Bereiche überschneiden um Doppelerfassungen zu verhindern.	Prinzipiell wurde darauf geachtet, dass keine Doppeleintragungen nötig und möglich sind.	Dies wurde durch relationale Verknüpfung der Stammdaten mit den verschiedenen Risikoeignern ermöglicht und führt zu einer häufigen gemeinsamen Verwendung von Einträgen. Umgesetzt ist das in den Arbeitsblättern Stammdaten indiv. Ereignisse, Stammdaten Ausprägungen und Stammdaten Maßnahmen erreicht.
BL-9	Das System bietet Schnittstellen um Daten austauschen (exportieren und importieren) zu können, siehe DB-5	Benötigt wird dies für z.B. Spezialsoftware, Berichte oder Excel Eigenauswertungen.	Minimum ist manuelle Schnittstelle mit .csv Tabellen.
BL-10	Das System berücksichtigt Interdependenzen zwischen den Risiken bei deren Aggregation. Siehe DB-10 und Abbildung 4.10.		Künftige Ausbaustufe. z.B. durch Varianz-Kovarianz-Methode möglich.
BL-11	Die Berichte müssen automatisiert generiert und an die zugeordneten Adressaten übermittelt werden. Siehe DB-13.		
BL-12	Die Risiken müssen durch Suchfelder und Sortierungen strukturiert werden können.	Such- und Filterfunktionen, siehe Abbildung 4.6.	
BL-13	Neue Risiken, individuelle Risiken, Ausprägungen oder Maßnahmen können im selben Risikoprozess Workflow eingegeben werden. Fließender Übergang zwischen Neubewertung und Neueingabe.	Das Arbeitsblatt in Abbildung 4.7 hinterlegt Stammdaten-Attribute in grau und ermöglicht erneute Eingabe von Bewegungsdaten.	Der Button "Neu Ausprägung"leitet zu einem ausklappbaren Bereich.

BL-14	Detailanalysen ausgewählter Risiken.	Eine detaillierte Beurteilung erfordert ein eigenes und speziell für das jeweilige Risiko erstelltes Arbeitsblatt.	Gestaltbare eigene Arbeitsblätter für spezielle Risikokategorien, wo neue Formeln und Daten verknüpft werden können, z.B. wie in Abbildung 4.11.
BO-1	Der User startet das Programm mit individuellem Startbildschirm.	Standardmäßig ist dies der komplette RM-Workflow mit Verlinkungen auf alle relevanten Arbeitsblätter und Programmbereiche.	Arbeitsblatt RM Workflow. Jedes Arbeitsblatt kann dafür eingestellt werden.
BO-2	Für jede Risikokategorie und deren konkrete Risiken müssen Maßnahmenpläne erstellt werden können.	Diese stellen das vorhandene Risikoausmaß dem durch Maßnahmen reduzierten gegenüber und sind mittels Aufwand, Kosten, Zeitplan und Umsetzung darstellbar.	Im Maßnahmenplan in DB-11 inkludiert.
BO-3	Für Risikokategorie, Unternehmensbereiche und konkrete Risiken können Risikolandkarten erstellt werden.	Risk maps werden zweifach verwendet. Erstens in Abbildung 4.15 als aggregierte Risikolandkarte. Zweitens im Risikoprozess laut Abbildung 4.9 um mittels Risikolandkarte auch einzelne Risiken mit Bedeutung und Häufigkeit zu visualisieren.	Risikolandkarte mit diversen Filtermöglichkeiten.

BO-4	Es muss ein Dashboard für jede Planungsebene (strategisch, taktisch und operativ) entworfen werden, da die Anforderungen der jeweiligen Anwender unterschiedlich sind.	Das Arbeitsblatt Reporting in Abbildung 4.15 zeigt eine Risikolandkarte für die Geschäftsführung. Im Risikoprozess sind Maßnahmenpläne nach Abbildung 4.13 und Übersichten in Abbildung 4.10 für die Risikoeigner vorgesehen.	Der Bereich Dashboard muss künftig noch verfeinert werden.
BO-5	Erklärungen und Erläuterungen können vom User während des Workflows eingesehen werden.	Ein- und ausblendbare Informationsabschnitte.	
BO-6	Für Berichte und zur Veranschaulichung der Risiken werden deren Ursache-Wirkungsketten betrachtet.	In Form von beschreibenden Textfeldern.	

Tabelle 6.1: Anforderungen für das Risikomanagement Informationssystem nach [Neuhauser(2011), vgl. Kp.6]

Die Umsetzung der in dieser Arbeit aufgebauten Anforderungen an ein Risikomanagement Informationssystem, siehe Tabelle 6.1, fand in Anlehnung an den beiden gängigen Werken ISO Norm und COSO II Framework statt. Zur Übersicht werden die Anforderungen entsprechend den 8 COSO Prozessschritten in Tabelle 6.2 zugeteilt. Das Ziel eines, nach sowohl COSO II als auch ISO31000, normgerechten Risikomanagement Informationssystems ist somit erfüllt.

COSO II RM-Prozessschritte nach Abschnitt 2.2	**Anforderungen nach Tabelle 6.1**
Internes Umfeld (RM-Philosophie, -Bereitschaft, ethische Werte und Leitsätze)	ORG-2, ORG-3, BL-5, BL-6, BO-5.
Geschäftsführung (Leitung)	ORG-3, BL-7.
Organisationsstruktur	ORG-4, DB-1, DB-2, BL-1, BL-4, BO-4.
Verantwortlichkeiten	DB-13, DB-14, DB-15, BL-1, BL-7, BO-1.
Zielfestlegung und daraus abgeleitete Risikobereitschaft und -toleranz	ORG-1, BL-7.
Einflussfaktoren	DB-6, DB-18, BL-2, BO-6.

Ereignisidentifizierungstechniken	DB-6, DB-7, DB-9.
Ereigniskategorien und Einteilung	ORG-4, DB-2, DB-3, DB-4, BL-12, BO-3.
Abhängigkeiten und Korrelationen	DB-4, DB-10, BL-8, BL-10.
Ermittlung Eintrittswahrscheinlichkeit und Bedeutung der Auswirkung	DB-6, DB-8, DA-17, BO-6.
Datenquellen	DB-5, BL-2, BL-9.
Bewertungsmethoden	DB-9, BO-3, BL-14.
Bewertung und Auswahl möglicher Steuerungsmaßnahmen	DB-11, BL-7.
Gesamtansicht mit Portfolio und Toprisiken	DB-11, BL-3, BL-10, BO-3.
Projektmanagement der RM-Maßnahmen	DB-11, BO-2.
Auswahl von Kontrollmaßnahmen	DB-12, DB-13, BL-6.
Regelungen und Verfahren	DB-12, BL-1.
Dashboard	BL-2, BO-2, BO-4.
Risikokommunikation	DB-2, DB-16, DB-17, BL-4, BL-7, BL-8, BL-12, BL-11, BO-1, BO-5.
Laufende Überwachungsmaßnahme	DB-12, DB-13, DB-17, DB-18, BL-7, BL-13.
Reporting	DB-13, DB-14, BL-11, BL-7.
Mängelberichterstattung	BL-6.

Tabelle 6.2: Verbindung der COSO RM-Prozessschritte mit den Anforderungen eines Risikomanagement Informationssystems

Als Hilfestellung zur strukturierten Erstellung der unternehmenseigenen Prozesslandschaft und zur Einbettung des Informationssystems in das vorhandene Managementsystem kann die [ONR(2014c)] dienen.

6.2 Designphase während der Software Entwicklung

Die Drei-Schichten Architektur, als etablierter Standard für Informationssysteme, wird verwendet, da die Systemgröße damit gut skalierbar ist und gleichzeitig einen hohen Grad an Flexibilität bei Anpassungen aufweist. Die klare Trennung der graphischen user-interface (Präsentationsschicht) von der Anwendungsschicht (2. Schicht) und die zentrale Datenhaltung der 3.Schicht, führen zu einer leichten Administration, siehe Abschnitt 5.3.

Die gesamten Daten werden, dem relationalen Datenmodell folgend, einheitlich in Tabellen dargestellt. Dies ist die weltweit verbreiteste Methode und wurde auch im Zuge des prevero Prototypen verwendet, wie in Abbildung 6.1 sichtbar:

Abbildung 6.1: Auszug aus der Präsentationsschicht, Anwendungsschicht und Datenschicht bei prevero p750

- Jede Tabelle ist eine, aus der Programmierung, bekannte Klasse (in prevero heißen diese Dimension)
- Jede Zeile der Tabelle entspricht einer Eintragung der jeweiligen, durch die Relation erfassten Dimension.
- Die Spalten der Tabellen entsprechen Eigenschaften (Attribute) einer Dimension.
- Tabellen werden durch einen eindeutigen Schlüssel identifiziert und verlinkt. Diese Verweisstrukturen zwischen den Tabellen werden vom Benutzer nicht gesehen.
- Modelle werden mittels entitiy-relation-model aufgebaut, siehe unten.

Datenbankmodel eines Risikomanagement Informationssystems nach Schwaiger

Das “Risiko Management Daten und Prozess Model” nach Schwaiger in Abbildung 6.2 gibt den Ausgangspunkt für die prototypische Entwicklung und orientiert sich an dem COSO II

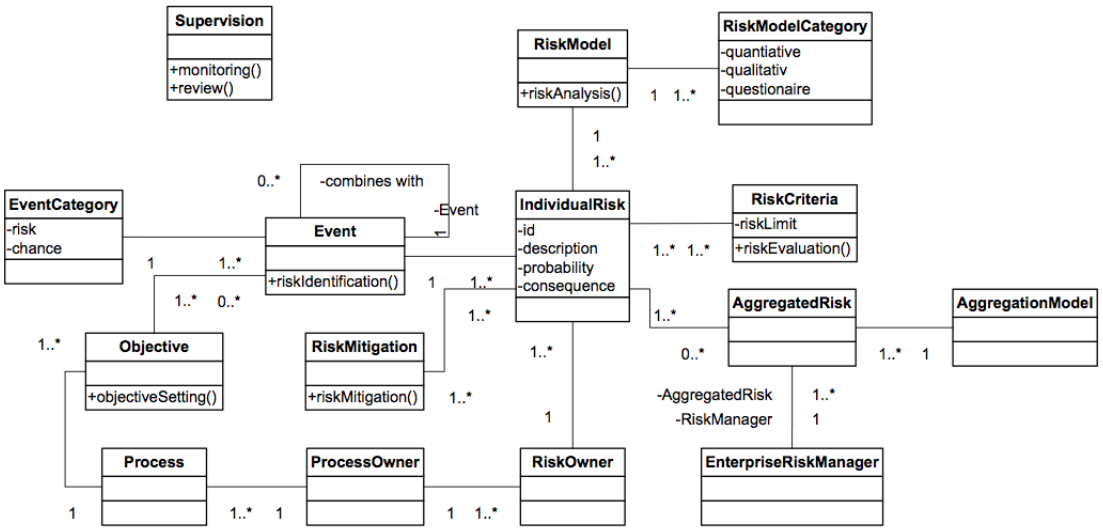


Abbildung 6.2: Generisches ERM Model für relationale Datenbanken nach [Schwaiger(2013)]

Risikomanagementsystem. Somit ist das Modell weitestgehend Branchenunabhängig und Normenkonform.

Erweitertes Datenbankmodell

Die Abbildung 6.2 wurde als Grundgerüst verwendet und im Zuge dieser Arbeit an die Erfordernisse des Projektpartners, als mittelständisches Industrieunternehmen, angepasst. Dabei ist die zentrale Frage jene nach dem passenden Datenmodell, als Grundlage für die Implementierung des Informationssystems!

Ausgehend vom Informationsfluss innerhalb des RM-Informationssystems nach [COSO(2009b), Exhibit 8.2] wurde folgendes erweiterte Datenbankschema entwickelt. Die Prämissen des Modells wurden für folgende Parameter entworfen:

Das hier beschriebene Risikomanagement Informationssystem Relationenmodell, wie etwa theoretisch in Abbildung 5.9 erklärt, kann als datenbankgerechtes Modell genutzt werden [Abts and Mülder(2013), vgl. S.165ff].

- Unternehmen die beim Aufbau ihres ERM Systems dem bottom-up Ansatz oder top-down folgen, können durch verschiedene Einstellungen das System spezifisch anpassen:
  - Je nach User der Software, sind andere Funktionen notwendig. Der hier gewählte Ansatz mit Ausprägungen ermöglicht, dass die Identifikation des Ereignisses (Risiko oder Chance) auf der untersteten Arbeitsebene stattfinden kann.

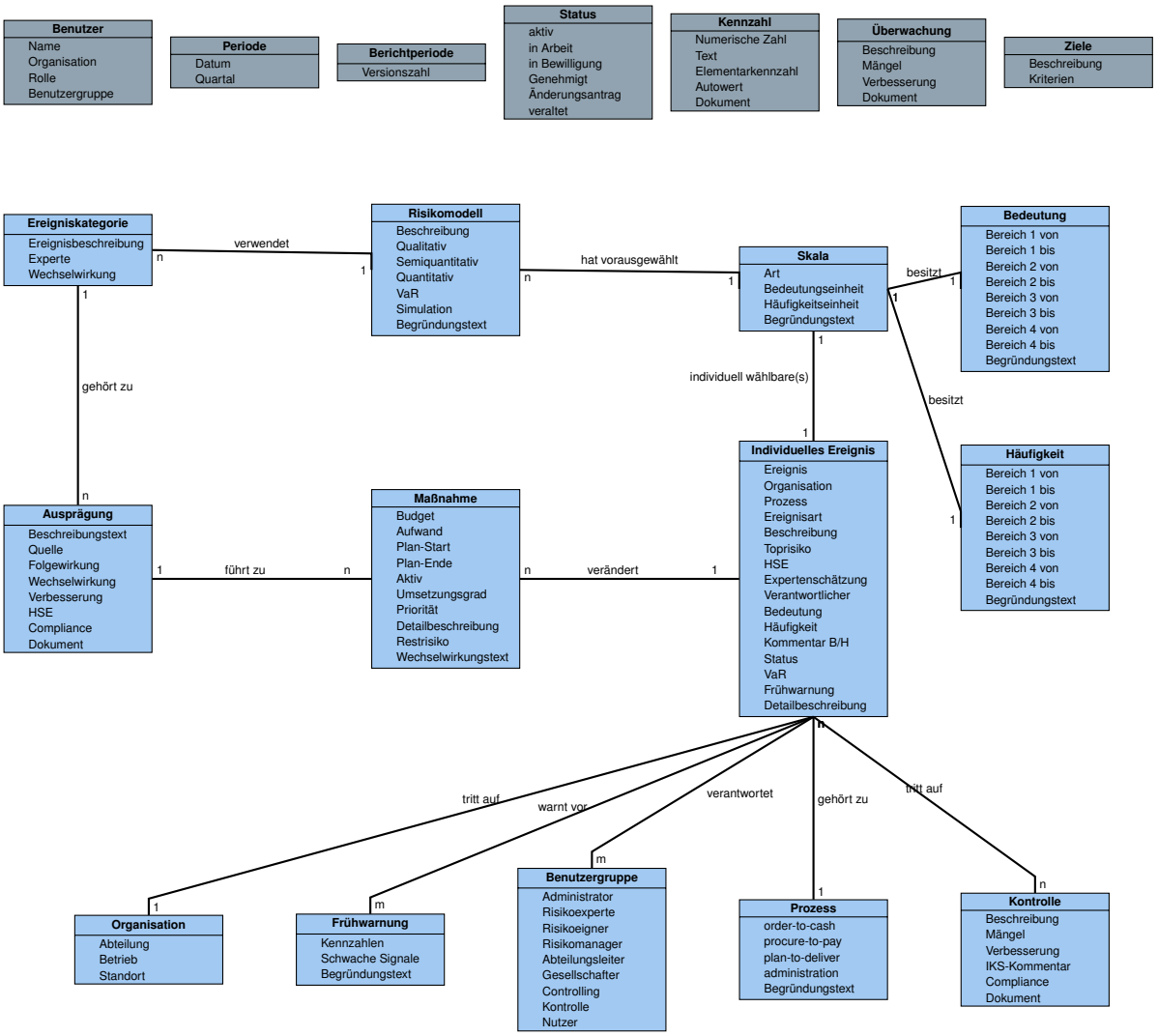


Abbildung 6.3: ER-Modell für ein industrielles Risikomanagement Informationssystem

  - Auch die Ereigniskategorien unterstützen das Einordnen und Wiederfinden von Sachverhalten bei einer breiteren Anwendungsbasis
  - Durch die Dimensionen Standort, Betrieb und Abteilungen ist das Aufschlüsseln und vergeben von Verantwortlichkeiten durchwegs granular gestalten.
  - Größtenteils zentral gesteuerte Unternehmen können durch Rollenvergabe eine zentrale RM Einheit mit allen Rechten ausstatten, siehe Dimension Enterprise-RiskManager.

- Dieses Model gibt die Möglichkeit ein ERM selbst zu entwickeln oder mit adaptierbaren business-intelligence Plattformen zu erweitern.

- Die grau hinterlegten Entitäten sind mit allen blau hinterlegten Entitäten n:m verknüpft. Diese Multidimensionalität ermöglicht eine nachverfolgbare Historie, simulierte Szenarien, Jahresabschlüsse, Detailanalyse einzelner Risiken, Detailergebnisse einzelner Organisationseinheiten, individuelle Benutzereinstellungen, parallele Bearbeitung mehrerer Nutzer, Statusvergabe und Hinterlegung verschiedener Daten und Kennzahlen pro Risiko.

- Die Kardinalität zwischen Maßnahme und individuellem Ereignis wäre bei Berücksichtigung von Korrelationen eine n:m Beziehung. Ebenso gilt dies zwischen Ereigniskategorie und Ausprägung und zwischen Ausprägung und Maßnahme. Die Korrelationen sind jedoch, wie im Abschnitt 3.7 beschrieben, nur mit hohem Reifegrad und Datenmengen berechenbar.

User Interface

Das Informationssystem wird anhand des im Kapitel 4 dargestelltem Risikomanagement und den im Abschnitt 6.1 beschriebenen Anforderungen gestaltet. Dabei sind insbesondere die nötigen Daten, vorhandene Datenquellen und andere bestehende Informationssysteme von Bedeutung und zu berücksichtigen.

- Start-Screen: Workflow des Risikomanagement mit Verlinkungen auf die jeweiligen Arbeitsblätter, Berichte, Übersichten, etc.

- Menü Verwaltung: Dies ist ein Standard Modul von prevero, welche Benutzerverwaltung mit Rollen und Rechten vorsieht.

- Stammdaten: Diese können bei prevero in den Dimensionen und Datenwürfel betrachtet werden.

- Risikoerfassung: Identifikation, Analyse der Bedeutung bzw. Häufigkeiten, Bewältigung mittels Maßnahmenplan und Kontrollen. Die Aggregation erfolgt durch die Risikokategorien und in der Risikomatrix. Jede Methode hat eine eigene Ansicht, zurzeit sind dies Fragebogen, VaR Berechnung oder Expertenschätzung.

- Risikoüberwachung und -kommunikation: Übersicht mittels Dashboard und Risikomatrix, Berichten und Periodenabschluss
- Dies soll eine Möglichkeit bieten, die historische Risikoentwicklung und deren Daten zu begutachten. Am besten als Zusatzfunktion mittels Perioden-Auswahl in den zuvor beschrieben Risikoansichten.

Dieser Grundversion folgend, wurde für den Konzern ein mehrteiliges und Datenbankunterstütztes Risiko Stammblatt erstellt, in seiner einfachsten Form als mock-up in Abbildung 6.4 dargestellt. Dieses mock-up wurde in Zusammenarbeit mit Christoph Aichinger erarbeitet. Die tatsächliche Umsetzung mittels prevero p7 ist im Risikomanagementhandbuch als Abbildung 4.7, Abbildung 4.9 bis Abbildung 4.12 erklärt. Dabei dient das Risiko Stammblatt im IT-System neben der Hauptfunktion als Benutzeroberfläche zusätzlich als taktgebender Workflow im Risikomanagementprozess.

Künftige Erweiterungen können folgende Ansichten beinhalten:

- Indikatoren-Hauptseite: Frühindikatoren, die regelmäßig manuell oder automatisch berechnet werden und somit Trends aufzeigen. Sie sind ein erstrebenswerter Teil.
- Korrelationen zwischen den einzelnen Risiken können mittels Korrelationsmatrix eingetragen werden, diese Werte sind jedoch ausschließlich mit datenreichem Zahlenwerk zu ermitteln.
- Schadensdatenbank, aller eingetretenen oder fast-eingetretenen Ereignisse, um die Expertenschätzungen ständig zu verbessern.
- Chancen-Management, die während des Risikomanagements genannten Ideen und Verbesserungsvorschläge aktiv managen.
- Risiken werden in deren Ursachen-Wirkungskette grafisch dargestellt oder modelliert.

6.3 Alternative zum Risikomanagement Informationssystem durch Nutzung bestehender Informationssystems

Dieses Kapitel zeigt die Möglichkeit das Risikomanagement innerhalb bereits etablierter, anderer softwareunterstützten Plattformen zu integrieren und dies nicht zwingend innerhalb eines neuen Informationssystems implementieren zu müssen. Denkbar wären etwa die Einbettung des Risikomanagements innerhalb bestehender Datenmanagementsystems oder prozessorientierter Managementsysteme (engl. business-process-system, kurz BPM, mehr dazu siehe Abschnitt 3.4).

Die folgenden Seiten zeigen das Beispiel der von Klaus Paier (Firma Rondo Ganahl AG) 2013 eigenentwickelten Softwarelösung. Diese nutzt die von den Anforderungen eines Prozessmanagement- bzw. Qualitätsmanagementsystems nach ISO 9001:2008 geforderten Prozesslandkarten als Ausgangspunkt für die Einpflege der Risiken und in weiterer Folge als Systemerweiterung die Behandlung innerhalb des Risikoprozesses.

Abbildung 6.4: Mock-up eines einfachen Risiko Stammblattes mittels Microsoft Excel 2011, [Denk(2008), vgl. Abb. 35 und 36]

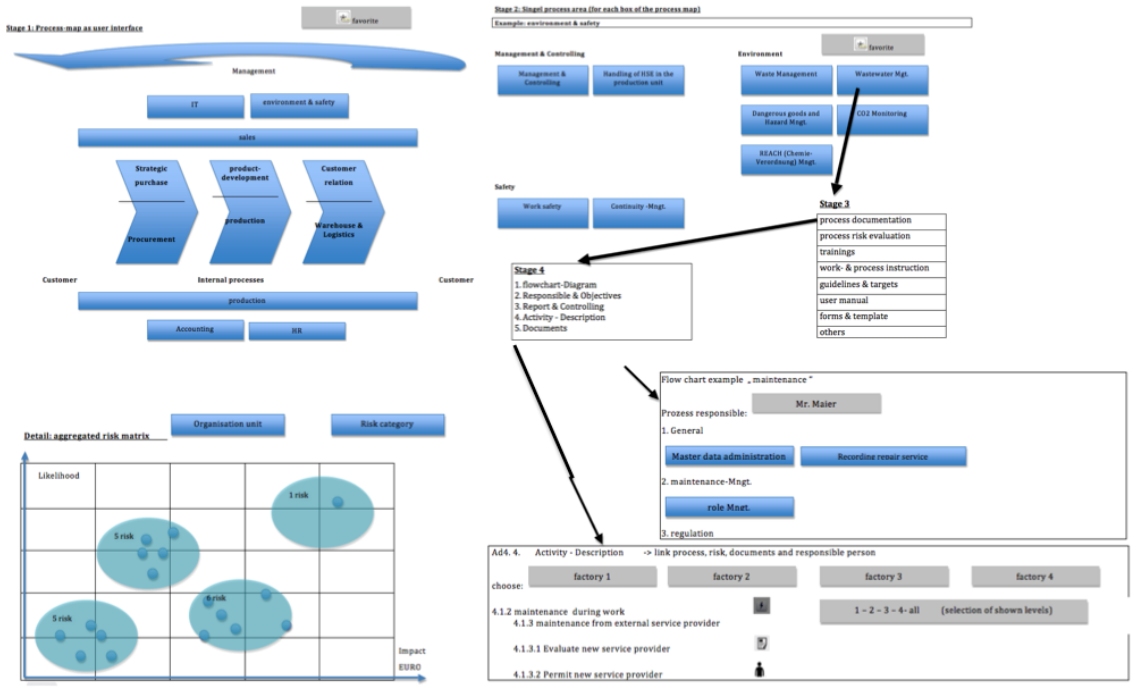


Abbildung 6.5: Konzept des Rondo Prozess- und Risikomanagementsystems nach Klaus Paier

Deren Zielstellung war die umfassende Prozessbeschreibung innerhalb einer professionellen Softwareplattform inklusive der vollständigen Risiken, unter Berücksichtigung der gewachsen Anforderungen und IT-Systeme.

Die Anforderungen des Rondo Prozessmanagementsystems setzen sich aus internen und externen Anforderungen zusammen. Interne Anforderungen an das Informationssystem sind etwa:

- Prozessstandards wie Transparenz, guter Benchmark, Einbindung des RM-Systems, Einhaltung der Compliance, etc.
- Abbildung der Organisation durch Verantwortliche und deren Stellvertreter
- Sicherung des unternehmenseigenen Knowhows durch Transparenz und Nachvollziehbarkeit der Abläufe
- Einschulung der Mitarbeiter

Externe Anforderungen:

- IKS als Anforderung der Wirtschaftsprüfer

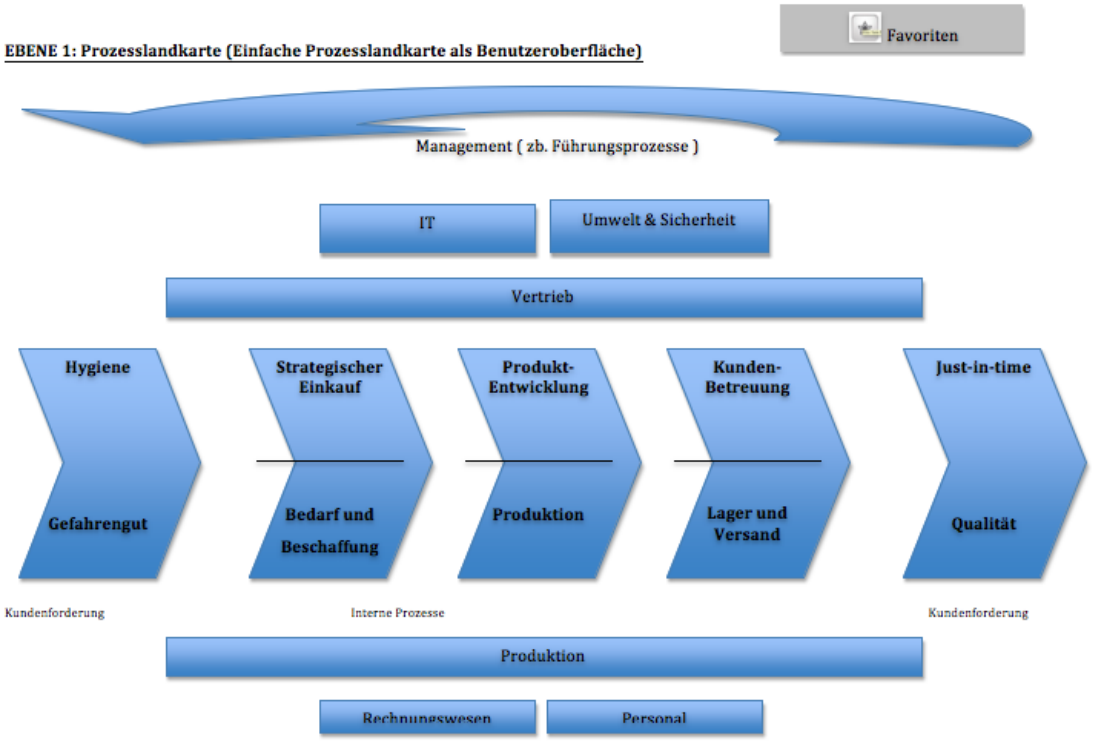


Abbildung 6.6: Rondo Prozess- und Risikomanagementsystem Ebene 1

- Verbesserungen durch die genaue Prozessdarstellung
- Das Informationssystem ersetzt bestehende Microsoft powerpoint-flowchart-diagramme und ermöglicht Ergänzungen und Erweiterungen
- Gesetzliche Anforderungen wie Rückverfolgbarkeit (bei Lebensmitteln), REACH (Chemie-Verordnung) oder ADR (Gefahrgut)
- Kundenanforderungen aus Branchen wie z.B. Lebensmittel, Pharma, Gefahrengüter steigen immerfort. Künftig sind vermehrt Risikoberichte mit gesetzten Maßnahmen gefordert, teilweise sogar schon FMEAs.

Die Softwareplattform und ihre Funktionen:

- Integration verschiedener interner Informationsmanagementsysteme (IMS) die jeweils eigene Dokumentationen haben, dies beinhaltet die Integration von:
  - Qualitätsmanagementsystem
  - Prozessmanagementsystem

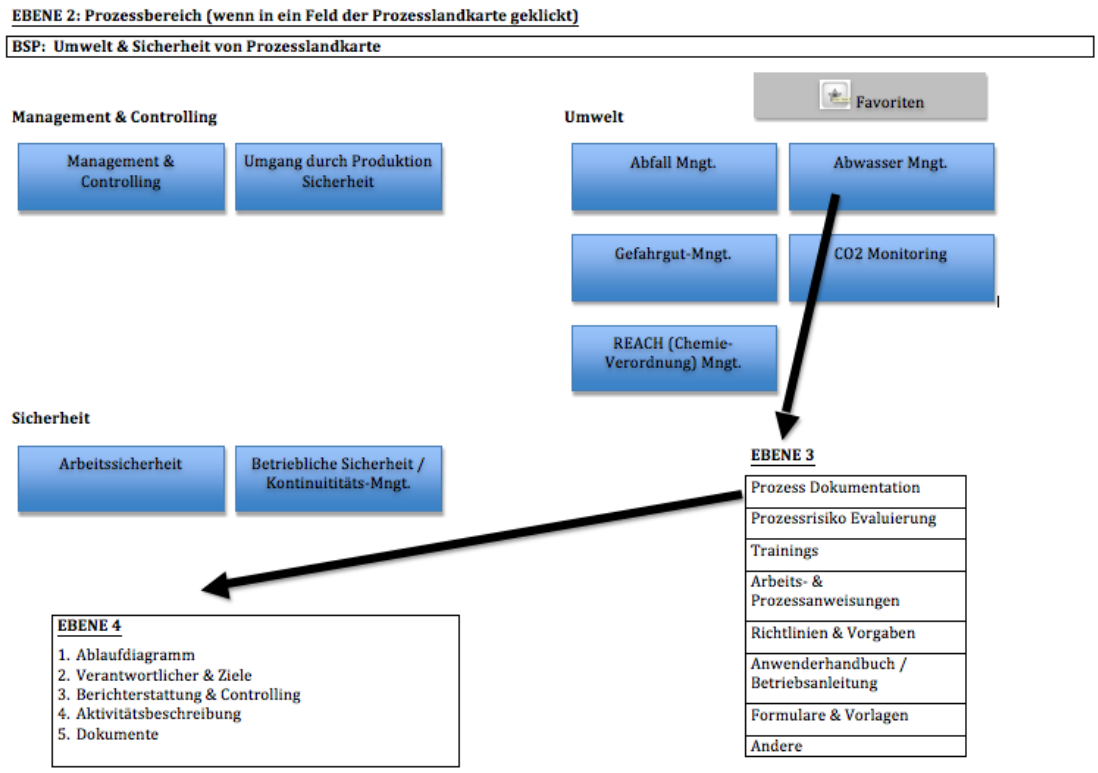


Abbildung 6.7: Rondo Prozess- und Risikomanagementsystem Ebene 2 und 3

  - Risikomanagementsystem mit Prozessrisiko Evaluierung, Maßnahmen, Verantwortlichkeiten, betrieblicher Sicherheit, Kontinuitätssystem, Risikokategorien und Risikobewertung
  - Umweltmanagementsystem
  - Arbeitssicherheitmanagementsystem
  - Zertifiziertes Managementsystem
- Prozess - und Risikoerhebung
  - Organisations-Abwicklung (interne Projektleiter)
  - Prozesserhebung mit Prozessverantwortlichen, Abläufen, Vorgaben, Richtlinien, Arbeits- und Prüfanweisungen, relevanten Dokumenten, Prozessrisiken
  - Klare Zuordnung der Prozess- und Risikoverantwortungen (Rollen und Verantwortungen können getrennt sein)
- Bereitstellung einer Softwareplattform
  - Informationsverwaltung

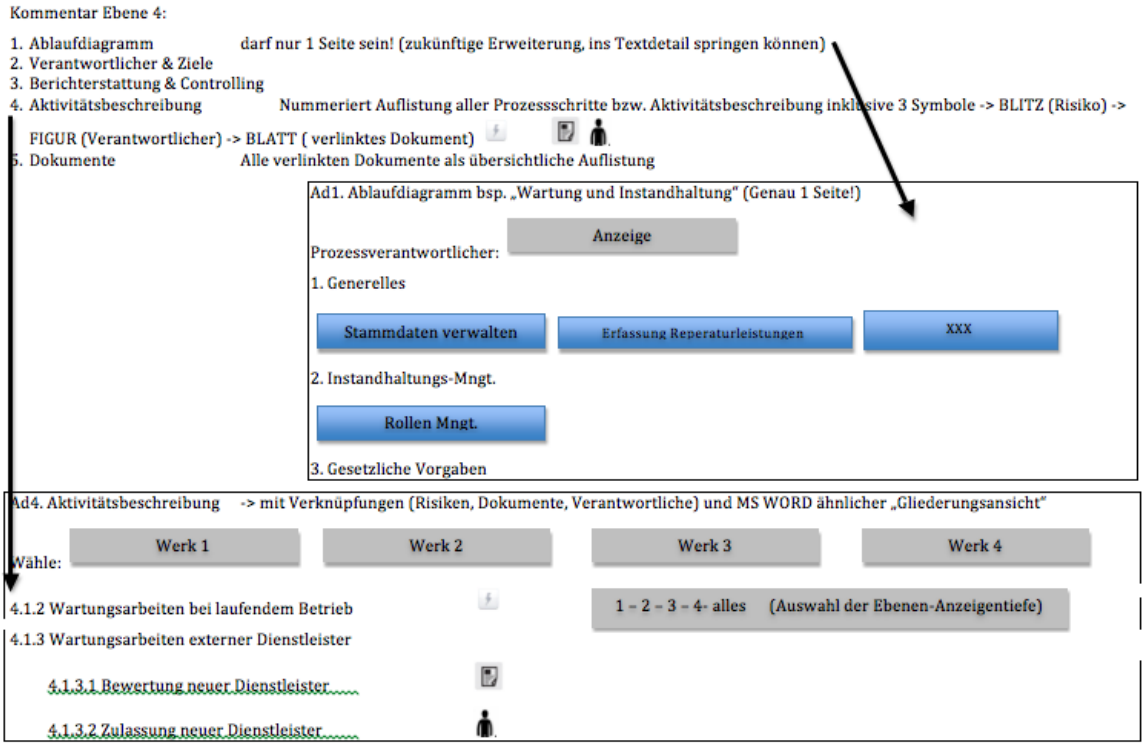


Abbildung 6.8: Rondo Prozess- und Risikomanagementsystem Ebene 4

- Unterteilung in (lokale) Systemadministration und power-user
- Erfassung der Prozessinformation als Historie
- Pflege und Änderungen der Inhalte bei Bedarf bedürfen Genehmigungsprozesse
- Bereitstellung des Systems für die Mitarbeiter

6.4 Alternative zum Risikomanagement Informationssystem durch bootstrapping

Bootstrapping steht im Englischen für eine funktionierende, provisorische und schnell fertiggestellte Minimallösung. Die Eingliederung des Risikomanagement Informationssystems kann in Anbetracht des heutigen Technologieumfangs dieser Systeme durchaus auch mit Standardsoftware oder innerhalb bestehender Individualsysteme ausreichen.

- Für Firmen die bereits Informationssysteme im Prozess-, Qualitäts- oder Datenmanagement nutzen oder bestehende Datenbanken mit risikorelevanten Daten haben, können eine schlichte Implementierung mit einigen wenigen Workflows und Benutze-

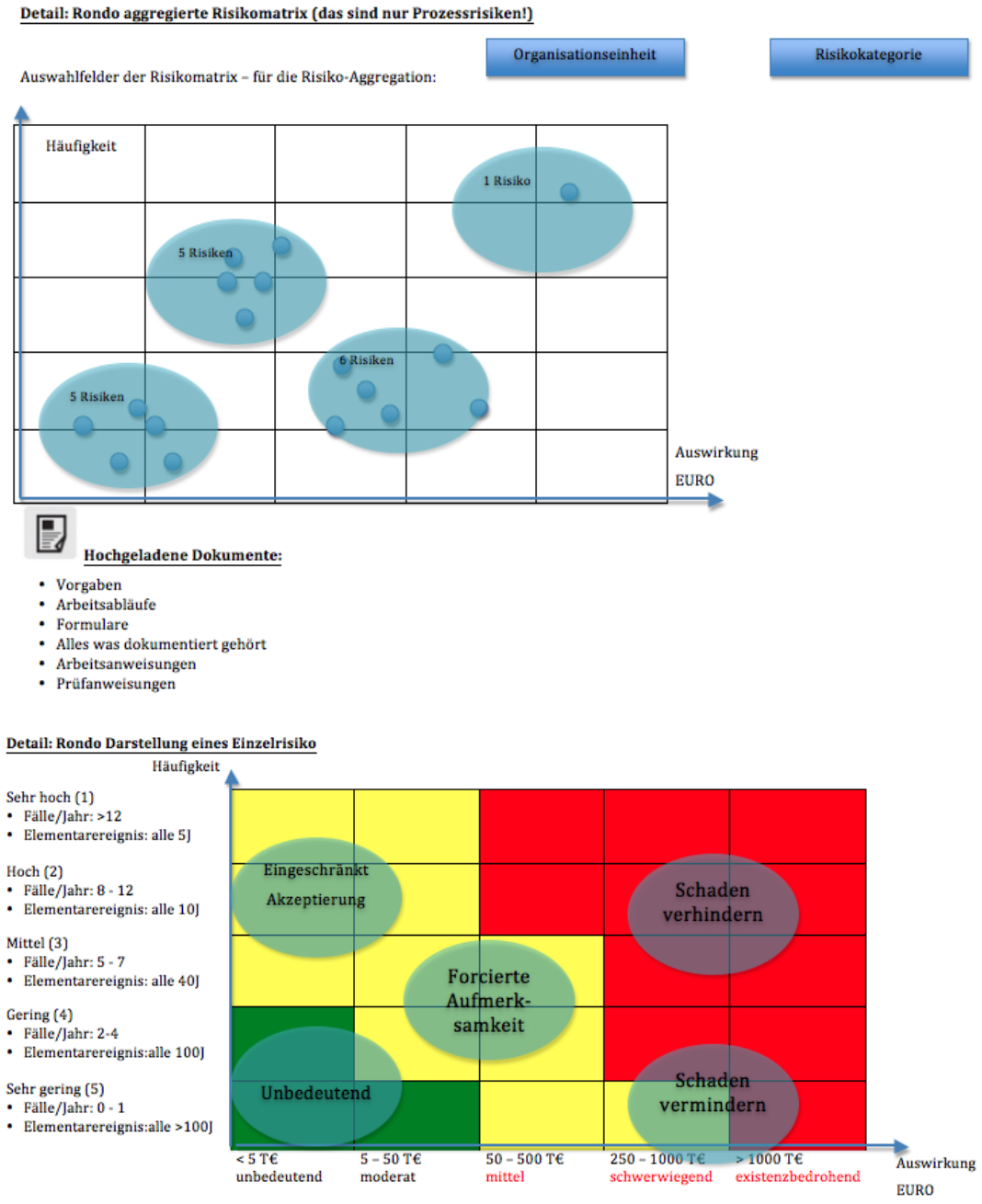


Abbildung 6.9: Rondo Prozess- und Risikomanagementsystem Risikobewertung

roberflächen selbst entwickeln. Diese Diplomarbeit stellt den Leitfaden diesbezüglich dar.

- Viele der in dieser Arbeit aufgelisteten Erfahrungswerte sprechen für die Nutzung einfach handhabbarer Excel-Tabellen mit automatisierbaren Makrofunktionen. Zumindest die Erstversion eines Risikomanagementsystems kann punkto Identifikation, Datensammlung, Analyse und Reporting durchaus in Microsoft Excel ausreichen. Der Grundgedanke am Risikomanagement lautet kontinuierliche Verbesserung und eine lebendige Risikokultur innerhalb des Unternehmens.

Gerade in KMUs löst jede zusätzliche Software einen Rattenschwanz an Schulungs-, Installations-, Nutzungsfrequenz, Anpassungswünschen etc. aus. Zu Beginn sind aber Risikobewusstsein und Schulungen wichtiger als eine hochmoderne Software.

Teil IV

Conclusion

KAPITEL 7

Conclusion

Einleitend wird das übergeordnete Ziel definiert, die Entwicklung eines unternehmensweiten und softwareunterstützten Risikomanagementsystems für einen mittelständischen Industriekonzern. Ausgehend von diesem Ziel wurden einzelne Teilziele abgeleitet, die nun einzeln diskutiert werden.

Ermittlung des aktuellen Industriestandards und der gesetzlichen Mindestanforderungen im Hinblick auf Risikomanagement

In Kapitel 2 wird diskutiert, dass vor allem zwei Entwicklungen der letzten Jahrzehnte die heutige Behandlung von Risiken verändert haben. Riesige Datensammlungen und billige Computer-Rechenleistung ermöglichten die Entstehung eines auf Risikoquantifizierung basierenden, automatisierten und softwareunterstützten Risikomanagementsystems.

Außerdem gaben sie einen Entwicklungsschub bei den Methoden, IT-Tools und Prozessen und änderten die Möglichkeiten des Risikomanagements in Richtung einer gesamtheitlichen Unternehmensbetrachtung.

Darauf aufbauend wird in Kapitel 3 jeweils auf die aktuellen Methoden des Risikomanagementprozesses und -rahmens detailliert eingegangen, wofür die Anwendung in führenden Branchen, diverse Normen, sowie Standardwerke der Literatur als Basis dienen. Daher stellt sich heraus, dass der aktuelle Industriestandard sehr heterogen ist und eine durchgängige Quantifizierung des Risikomanagementprozesses weder gesetzlich gefordert ist, noch gängiger Praxis entspricht. Außerdem wird die bis dato gängige Annahme, dass es in Industrieunternehmen genügt, mit statistischen Methoden Risiken adäquat behandeln und kontrollieren zu können, zunehmend in Frage gestellt. Stattdessen ist es unbedingt notwendig, zuvor den Risikomanagementrahmen zentral im Bewusstsein der Führungskräfte und Mitarbeiter zu verankern, wofür ein hohes Maß an sozialer Kompetenz und Ausdauer benötigt wird. Erst nach erfolgreicher Implementierung eines solchen Risikomanagementrahmens ist es ratsam - falls die notwendigen Ressourcen vorhanden sind - ein komplexes mathematisches Modell schrittweise einzusetzen.

Um verschiedene mögliche Ausbaustufen eines Risikomanagementsystems übersichtlich darzustellen, wird im Kapitel 4 ein eigenes Reifegradmodell entwickelt. Ein Reifegrad der Stufe 1 (von 4) mit einer simplen Herangehensweise ist sowohl aus gesetzlicher als auch unternehmerischer Sicht nicht mehr ausreichend und muss mindestens durch eine strukturierte Herangehensweise der Stufe 2, die den gesetzlichen Mindestanforderungen entspricht, ersetzt werden.

Entwicklung eines unternehmensweiten und regelkreisgesteuerten Risikomanagementsystems ausgehend von den Bedürfnissen eines mittelständischen Industriekonzerns

Für die Anwendung eines Risikomanagementprozesses und -rahmens wird in Kapitel 3 ein Anwendungsleitfaden erstellt. Dieser liefert zu jedem Prozessschritt verschiedene grundlegende Ansätze und Methoden zur Auswahl. Je nach spezifischen Verhältnissen im Unternehmen können so die passenden Instrumente ausgewählt werden, um das Risikomanagementsystem so genau wie möglich an die Charakteristika des Unternehmens anzupassen.

Sowohl in der Theorie als auch in der Praxis sind die beiden schwierigsten Fragestellungen des Risikomanagementprozesses jene der Quantifizierung und der Aggregation von Risiken.

Für die bestmögliche Beantwortung dieser Fragestellungen ist eine umfangreiche Datenbasis notwendig. Bis auf wenige Ausnahmen verfügen Industriebetriebe jedoch meist nur über unzureichende Daten zu Schadensfällen, weshalb die Anwendung fast aller mathematisch-statistischen Risikoanalyseverfahren nicht sofort möglich ist, um das Risiko nachvollziehbar und zuverlässig abzuschätzen. Eine ebenfalls aufwändige, aber für den mittelständischen Industriebetrieb machbare Möglichkeit für die Quantifizierung und Aggregation ist die Verwendung von semiquantitativen Methoden, wie Risikolandkarten und Expertenschätzungen.

Das in Kapitel 4 erstellte Modell bedient sich deshalb ebenfalls aufwändiger, aber für den mittelständischen Industriebetrieb machbarer, semiquantitativer Methoden. Die Risikoquantifizierung erfolgt innerhalb einer Risikolandkarte mit 16 Feldern und zusätzlich einer erneuten Expertenschätzung zur Ermittlung der Toprisiken für die Geschäftsleitung. Die Aggregierung des Risikos erfolgt durch eine, im Zuge dieser Arbeit entwickelte Risikokategorisieung, inklusive dazugehörigem Risikokontenplan, um eine Zusammenfassung oder Filterung von Hierarchieebenen, Verantwortlichen, Ländern, Unternehmensbereichen oder Risikokategorien zu bewerkstelligen.

Der Anwendungsleitfaden gibt weiters Antwort darauf wie Risikomanagement am besten in Unternehmen eingegliedert wird. Hierfür wird eine Risikopyramide entwickelt, die das Risikomanagement mit Hilfe von Kennzahlensystemen in die Unternehmenshierarchie einbettet. Außerdem wird das in der Praxis gängige three-lines-of-defense Modell herangezogen, um eine mehrstufige Rollenverteilung im Unternehmen herzustellen.

Einführung eines normgerechten Risikomanagementsystems in einem mittelständischen Industrieunternehmen

Die Einführung eines normgerechten Risikomanagementsystems in einem mittelständischen Industrieunternehmen kann durch die Erstellung eines Risikomanagementhandbuchs, die Abhaltung von Workshops, die Anbindung an ein bestehendes Prozessmanagementsystem, sowie die Implementierung eines softwareunterstützten Informationssystems erfolgen.

In Kapitel 4 wird zur Erreichung dieses Teilziels ein Risikomanagementhandbuch erstellt, da dies mehrere Vorteile mit sich bringt: Erstens eignet sich ein Risikomanagementhandbuch gut für die Einführung von Risikomanagement im Unternehmen, da es eine ganzheitliche Einbindung in allen Bereichen ermöglicht. Zweitens stellt es eine gute Grundlage für einen weiteren Ausbau des Risikomanagements durch komplexere Systeme, wie etwa ein softwareunterstütztes Informationssystem, dar. Außerdem ist die Anwendung eines solchen Handbuchs gängige Praxis in mittelständischen Industrieunternehmen.

Die Struktur des vorliegenden Risikomanagementhandbuchs folgt beiden gängigen Normenwerken COSO II Enterprise Risk Management Framework und ISO 31000 und ist an mehreren best-practice Methoden angelehnt. In verschiedenen Kapiteln werden die wichtigsten Elemente eines Risikomanagementsystems wie folgt behandelt:

- Erläuterungen der Grundsätze und verwendeten Begriffe des Risikomanagements und deren strategische Vorgaben in Form der Risikomanagementpolitik in Kapitel 0 und 1.
- Kapitel 2 dient zur Regelung der Aufbau- und Ablauforganisation, Kompetenzordnung und der Verantwortlichkeiten. Schnittstellen zwischen dem Risikomanagement und anderen Abteilungen werden erläutert.
- Kapitel 3 beschreibt die verpflichtenden Methoden und Risikoprozesse im Unternehmen, hinsichtlich Einteilung der Risiken in Kategorien, Risikokontoplan, Ausgestaltung von Prozessen für die Risikobewertung, Risikosteuerung, Risikoberichterstattung und Kommunikation.
- Kapitel 4 zeigt die Umsetzung des Risikomanagementsystems mittels Software.
- Schließlich legt Kapitel 5 die Geltungsbereiche, Inkraftsetzung, gesetzliche Regelungen und Versionierungen fest.

Das Abschnitt 3.2 kann außerdem als Vorlage für andere mittelständische Unternehmen dienen.

Weiterentwicklung des Risikomanagements durch ein softwareunterstütztes Informationssystem

Die Weiterentwicklung des Risikomanagements durch die Einführung eines softwareunterstützten Informationssystems kann entweder auf einem Standard IT-System basieren, oder durch eine Eigenentwicklung erfolgen. Da ein, für die Bedürfnisse eines mittelständischen Industriekonzerns zufriedenstellendes Standardsystem am derzeitigen Softwaremarkt nicht verfügbar ist, wird ein eigenes System entwickelt.

Hierfür werden in Kapitel 5 und 6 zuerst die Anforderungen und Funktionen für ein softwareunterstütztes Risikomanagementsystem ermittelt. Die umfangreichen Anforderungen wurden in die vier Komponenten Datenbank, business-intelligence, user-interface und Organisation gegliedert. Diesen Komponenten werden 42 Funktionen zugeordnet, die im Zuge des Prototyps umgesetzt und bewertet werden, siehe Tabelle 6.1.

Weiters wird der Prototyp eines softwareunterstützten Risikomanagementsystems als Anwendungssystem entwickelt, welcher dem Modell eines analytischen Informationsmanagementsystems nach Krcmar folgt. Dieses Informationsmanagementsystem basiert auf drei Ebenen (Informationswirtschaft, Informationssystem und technisches Basissystem) und seine Hauptaufgabe ist die betriebswirtschaftlich sinnvolle Steuerung der Ressource Information. Die technische Umsetzung erfolgt mittels der 3-Schichten-Architektur:

- Die Datenbankschicht erklärt die Erstellung eines risikospezifischen Datenmodells mittels Relationenmodell und die generelle Handhabung von Daten.
- Die Verarbeitungsschicht dient der Datenanalyse mittels mehrdimensionalen Kennzahlen (OLAP) und mathematischen Modellen.
- Die Präsentationsschicht geht auf die Prinzipien der Benutzerschnittstellen bzw. -oberflächen ein.

Beiträge dieser Arbeit

In Abschnitt 4.8 werden die in den einzelnen Projektphasen gemachten Erfahrungen, Ideen, Probleme und Lösungen zusammengefasst. Sie können als Ausgangspunkt und Anregung für Risikomanager eines mittelständischen Industriebetriebes oder weiterführende Forschungsprojekte gleichermaßen dienen.

Der wissenschaftliche Beitrag in dieser Arbeit umfasst:

- Ein Modell zur Risikokategorisierung inklusive Risikokontorahmen zur übersichtlichen Behandlung vieler Risiken in großen Unternehmen.
- Das Modell in Abbildung 3.1 verbindet das unternehmensweite Risikomanagement in seiner Natur als Strategieprozess inklusive change-management und als große Risikokalkulation.

- Eine mittelständische Organisationsstruktur im Unternehmen wurde entwickelt.
- Ein umfangreiches Reifegradmodell zur Bewertung des Risikomanagements wurde aufgebaut.
- Eine einfache Risikoberechnung in Form von Quantifizierung und Aggregation mittels Risikolandkarten wurde, mit Rücksicht auf typische mittelständische Datenquellen und Methodenkenntnisse, entwickelt.
- Ein Risikomanagement Datenmodell, das durch die Einführung von individuellen Risiken und Ausprägungen eine individuelle Benutzung ermöglicht. Die Verknüpfung vieler Funktionen erfolgte im Datenmodell generisch mit denen der Kategorien, dies reduziert die Wartungsarbeiten und Fehlerquellen der Administratoren.
- Die Gestaltung der Benutzeroberfläche als übersichtlicher Workflow in der Navigation und im Risikomanagementprozess. Die Berichte wurden als Managementcockpits gestaltet.

Diese Arbeit ist für den Einsatz in mittelständischen Unternehmen gedacht, daher wird großer Wert auf umfangreiche Beispielsammlungen und Vorlagen gelegt.

Ausblick auf künftige Forschungsfelder

Bei der Einführung eines unternehmensweiten Risikomanagements sollten die Gedanken des österreichischen Wissenschaftlers Gottfried Schatz im Kopf behalten werden. Schatz führt aus, dass die großen Probleme unserer heutigen Gesellschaft mit Technik alleine nicht lösbar sind. Die Probleme sind sozialer und politischer Natur, daher ist es wichtig die Wissenschaft nicht nur als Quelle neuerer Geräte oder wirtschaftlichen Wachstums zu sehen. Wissenschaft ist mehr als nur Wissen, es ist auch Bescheidenheit, Vernunft und der Mut zum eigenen Denken [1]. Die Naturwissenschaftlichen Methoden haben erstaunlich wenig zum beiliegenden Projekt beigetragen. Es sind vielmehr Softskills als weiche Faktoren und weiche Einflüsse von Risikokultur bis Transparenz und die Aufbereitung und Auswertung von Informationen, die wesentlich für den Erfolg eines Risikomanagementsystems verantwortlich sind. Und genau diese weichen Faktoren bieten Forschungsmöglichkeiten für empirische Studien oder Modellentwicklungen die das Risikomanagement besser im Unternehmen verknüpfen können. Auch nach dieser Arbeit muss weiterhin nach einem akzeptablem Modell aus technischen und mathematischen Methoden geforscht werden, nach dem Motto “so wenig wie möglich und so viel wie nötig”.

Bei rein technischer Betrachtung fallen folgende notwendige Forschungsfelder im Risikomanagement auf:

[1] https://medienportal.univie.ac.at/videos/650-jahr-jubilaeum/detailansicht/artikel/eroeffnungsfestakt-der-festvortrag-von-gottfried-schatz/ (12.10.2015)

- Berücksichtigung von Risikointerdependenzen sowohl zwischen Risiken, Maßnahmen und Zielen. So konnten im Kapitel 4, Aufgrund von Datenarmut, aus den 880 Risiken keine mehrfachen Zuordnungen bei den Risikokategorien vollzogen werden. Durchschnittlich hätte jedes Risiko in 1,64 Kategorien zugeteilt werden können, wobei 484 Risiken mit 2 Kategorien und 42 sogar mit 3 Kategorien Interdependenzen gehabt hätten.

- Eine Verbindung zwischen Risikomanagement und der Unternehmenssteuerung mit bestehenden Organisations-, Planungs- und Berichtssystemen (insbesondere Controlling-, balance-score-card- oder Qualitätsmanagementsysteme) wird allerseits gewünscht. Schnittstellen zwischen artverwandten Tätigkeiten und Abteilungen, wie es in dieser Arbeit oder bei [Schleinzer(2014)] unterfangen wurde, können als Ausgangspunkt dienen. Ebenso eine reibungslose und automatisierte Methode die Risikoprozesse in die vorhandenen Prozesse zu integrieren. Der derzeitige Aufwand ist enorm und muss oft individuell pro Unternehmen ausgelegt werden! Einher geht die Frage nach bestmöglicher Integration der Risikoziele in die Unternehmensziele. Ein Vergleich der Ergebnisse dieser Arbeit mit Studien in Abschnitt 4.9 und alternativen Modellen in Abschnitt 4.9 wurde nur oberflächlich begangen.

- Es fehlen Studien und best-practice Methoden zur Identifikation, Messung, Berechnung und Aggregation der Risiken in mittelständischen Industrieunternehmen.

- Die Erschaffung von allgemeinen Datenbanken mit quantifizierten Risikodaten oder Verlustdatenbanken aus unternehmensübergreifenden Quellen ist dringend nötig. Diese Daten fehlen zur Analyse vieler Risikokategorien.

Bezüglich der Entwicklung von Informationssystemen für das Risikomanagement können folgende Fragen künftig von Interesse sein:

- Möglichkeiten das Risikomanagement innerhalb bereits etablierter anderer softwareunterstützen Plattformen zu integrieren und dies nicht zwingend innerhalb eines neuen Informationssystems implementieren zu müssen. Denkbar wären etwa die Einbettung des Risikomanagements innerhalb der prozessorientierten Managementsysteme (siehe Abschnitt 3.4 und Abschnitt 6.3) und dessen BPMS (engl. business-process-management-system). Auch innerhalb von Projektmanagementsystemen könnte diese Integration erfolgen, so hat der PMBOK Guide nach [PMI(2014)] ein eigenes Kapitel für project-riskmanagement und die pm baseline nach [IPMA et al.(2006)] behandelt Projektrisiken und Projektportfoliorisiken. Innerhalb dieser Fragestellung wäre eine breiträumige Identifikation von bestehenden Plattformen und anschließendem Vergleich der Brauchbarkeit innerhalb der verschiedenen Funktionen des Risikomanagements eine wichtige Forschungsfrage.

- Die Erstellung von Vorlagen und/oder Beurteilung von bootstrapping Methoden (engl. für Umsetzung mit minimalen Mitteln) ist als Fragestellung besonders für Mittelständische Unternehmen angebracht! Die Umsetzung eines Risikomanagementsystems

mittels cloud-basierenden-online-Plattformen wären kostengünstig oder open-source. Diese können von reinen webbasierten Projektmanagement Plattformen wie z.B. basecamp bis zu den weitverbreiteten simplen kollaborativen Tabellenkalkulationsprogrammen wie z.B. Microsoft Office 365 oder googledocs reichen.

- Interessant wäre auch collobaration-Plattformen wie GitHub als Basis einer Adaptierung für die Zwecke einer Risikomanagementplattform zu nutzen.
- Es gibt hunderte webbasierte Entwicklungsplattformen für Software [2]. Diese bieten eine Infrastruktur die viele der technischen Voraussetzungen ermöglicht, etwa kollaborative Versionsverwaltung, Kommunikation (Diskussion, Blogs, Wikipedia, web-publishing, Kommentare, Umfragen), Fehlerverwaltung (issue-tracking), Zeitplanung (Kalender, time-tracking), Projekt-Portfoliomanagement, Ressourcenmanagement, Dokumentenmanagement, workflow-system, Reporting, Rollenverteilung, Zugriffsregelungen und technische Analyse (business-intelligence, charting, tagging, rating).
- Einige Vorteile liegen auf der Hand: Die Unabhängigkeit gegenüber lock-in Effekten, Vermeidung von spezifischen Funktions- oder Prozessvorgaben, gängige Programmiersprachen (konträr zu ABAP bei SAP), kostengünstige Anschaffung oder ausgereifte Benutzeroberflächen und Grundfunktionen.
- Die Nachteile bei einer Abbildung der Risikomanagementfunktionen innerhalb einer generischen Plattform oder online Tabellenprogrammen sind der ebenfalls hohe Aufwand, der möglicherweise einer Eigenentwicklung nahe kommt. Es würde sich um eine stand-alone Software für das Risikomanagement handeln, die wahrscheinlich keine integrierte Firmenlösung aller IT-Aufgaben ermöglicht. Die Datenhoheit befindet sich wie bei den meisten mittelständischen Softwarelösungen nicht mehr im Unternehmen, sondern in der cloud des Anbieters. Letztlich sollten Überlegungen erfolgen, ob mögliche Versionierungen des Anbietersystems die eigenen Prozesse gefährden würden.

[2] `https://en.wikipedia.org/wiki/Comparison_of_project_management_software` und `https://en.wikipedia.org/wiki/List_of_collaborative_software` (13.11.2015)

Literaturverzeichnis

[Abts and Mülder(2013)] D. Abts and W. Mülder. *Grundkurs Wirtschaftsinformatik. Eine kompakte und praxisorientierte Einführung*. Vieweg+Teubner Verlag, 2013. ISBN 9783322942845. URL https://books.google.at/books?id=4IT4BQAAQBAJ.

[accenture(2011)] accenture. Report on the accenture 2011 global risk management study, 2011.

[accenture(2013)] accenture. Insights into risk management - how it works in practice! TU WIEN - Vorlesung Enterprise Risk Management Fundamentals 19.4.2013, 2013.

[Ansoff(1975a)] H. I. Ansoff. Managing strategic surprise by response to weak signals california management review. pages 21–33, 1975a.

[Ansoff(1975b)] H. Igor Ansoff. Managing strategic surprise by response to weak signals. *California Management Review*, 18(2):21–33, 1975b.

[Bacher(2004)] Martin Bacher. Die eignung von value-at-risk-systemen zur risikosteuerung in nicht-finanzdienstleistungsunternehmen, 2004.

[BaFin(2011)] Bundesanstalt für Finanzdienstleistungsaufsicht BaFin. Aufsichtliche beurteilung bankinterner risikotragfähigkeitskonzepte, 2011. URL http://www.bundesbank.de/Redaktion/DE/Standardartikel/Aufgaben/Bankenaufsicht/risikomanagement_marisk_risikotragfaehigkeit.html.

[Basel(2009)] Committee on Banking Supervision Basel. Results from the 2008 loss data collection exercise for operational risk, 2009.

[Basel(2010a)] Committee on Banking Supervision Basel. Developments in modelling risk aggregation, 2010a.

[Basel(2010b)] Committee on Banking Supervision Basel. Developments in modelling risk aggregation, 2010b.

[Basel(2011)] Committee on Banking Supervision Basel. Operational risk-supervisory guidelines for the advanced measurement approaches, 2011.

[bdi and pwc(2011)] Bundesverband der Deutschen Industrie e.V. bdi and PricewaterhouseCoopers AG pwc. Risikomanagement 2.0: Ergebnisse und empfehlungen aus einer befragung in mittelständischen deutschen unternehmen. 2011.

[Becker(2005)] T. Becker. *Prozesse in Produktion und Supply Chain optimieren*. Springer Berlin Heidelberg, 2005. ISBN 9783540258414. URL https://books.google.at/books?id=z4mP1f22gjMC.

[BFI(2006)] Fachhochschule des bfi GMBH BFI. Risikomanagement in unternehmen. 2006. ISSN 18129064.

[Biffl(2010)] Stefan Biffl. Software-qualitaetssicherung vorlesungsübung block 1. Vorlesung 180.764 Software-Qualitätssicherung, 2010.

[Bokesch(2012)] Gregor Bokesch. Risikoberichterstattung in österreichischen und deutschen kapitalmarktorientierten konzernabschlüssen (atx, dax, 2007 bis 2010) - auswirkungen der finanz- und wirtschaftskrise, 2012. Linz, Univ., Dipl.-Arb., 2012.

[Bouder and Slavin(2013)] F. Bouder and D. Slavin. *The Tolerability of Risk: A New Framework for Risk Management*. Taylor & Francis, 2013. ISBN 9781136551819. URL https://books.google.de/books?id=VdqAAAAAQBAJ.

[Bourque and Fairley(2014)] Pierre Bourque and Richard E. Fairley. *Guide to the Software Engineering Body of Knowledge (SWEBOK)*, volume 3.0. IEEE Computer Society Press, 2014.

[Brodeur(August 2010)] Andre Brodeur. Top-down erm: A pragmatic approach to managing risk from the c-suite. (22), August 2010.

[Brösel(2004)] G. Brösel. *Internationale Rechnungslegung, Prüfung und Analyse: Aufgaben und Lösungen*. Studien- und Übungsbücher der Wirtschafts- und Sozialwissenschaften. Oldenbourg, 2004. ISBN 9783486275964. URL https://books.google.at/books?id=4VNK4qAwxbYC.

[Brühwiler and Romeike(2010)] B. Brühwiler and F. Romeike. *Praxisleitfaden Risikomanagement; ISO 31000 und ONR 49000 sicher anwenden*. Erich Schmidt, Berlin, 2010. ISBN 978-3-503-12476-3.

[Bungartz(2012)] O. Bungartz. *Handbuch Interne Kontrollsysteme (IKS): Steuerung und Überwachung von Unternehmen*. Compliance digital. 2012. ISBN 9783503136728. URL https://books.google.de/books?id=hfHZDmATE7sC.

[Christian and Lüdenbach(2013)] D. Christian and N. Lüdenbach. *IFRS Essentials*. Wiley Regulatory Reporting. Wiley, 2013. ISBN 9781118501344. URL https://books.google.at/books?id=8b6zFka3hUwC.

[COSO(2006)] Committee of Sponsoring Organizations of the Treadway Commission COSO. Internal control over financial reporting - guidance for smaller public companies, 2006. www.coso.org.

[COSO(2009a)] Committee of Sponsoring Organizations of the Treadway Commission COSO. Enterprise risk management - integrated framework, 2009a. www.internerevision.at.

[COSO(2009b)] Committee of Sponsoring Organizations of the Treadway Commission COSO. Enterprise risk management - integrated framework - anwendungsleitfaden, 2009b. www.internerevision.at.

[Cruz(2004)] Marcelo Cruz. *Operational risk modelling and analysis : theory and practice*. 2004. ISBN 1-904339-34-4.

[Curtis and Carey(2012)] Patchin Curtis and Mark Carey. Risk assessment in practice. 2012.

[Damodaran(2008)] A. Damodaran. *Strategic Risk Taking: A Framework for Risk Management*. Wharton School Pub., 2008. ISBN 9780131990487. URL `http://books.google.at/books?id=TJ0dnfed0_wC`.

[Denk(2008)] Robert Denk. *Corporate Risk Management; unternehmensweites Risikomanagement als Führungsaufgabe*. Fachbuch Wirtschaft. Linde, Wien, 2., überarb. und erw. aufl. edition, 2008. ISBN 978-3-7143-0138-0.

[DGR(2008)] Deutsche Gesellschaft für Risikomanagement DGR. *Risikoaggregation in der Praxis. Beispiele und Verfahren aus dem Risikomanagement von Unternehmen*. Springer, Berlin [u.a.], 2008. ISBN 978-3-540-73249-5; 3-540-73249-7.

[Diebold et al.(2010)Diebold, Doherty, and Herring] Francis X. Diebold, Neil A. Doherty, and Richard J. Herring. *The known, the unknown, and the unknowable in financial risk management: measurement and theory advancing practice*. Princeton University Press, 2010.

[Diederichs(2012)] Marc Diederichs. *Risikomanagement und Risikocontrolling*. Finance competence. Vahlen, Muenchen, 3.aufl. edition, 2012. ISBN 978-3-8006-4222-9; 3-8006-4222-0. Teilw. zugl.: Dortmund, Univ., Diss., 2003.

[DIN and IEC(2001)] Deutsches Institut für Normung e. V. DIN and Internationale Elektrotechnische Kommission) IEC. Din iec 62198 risikomanagement für projekte anwendungsleitfaden, 2001.

[Drucker(1964)] Peter Ferdinand Drucker. *Managing for results: economic tasks and risk-taking decisions*. Routledge, 1964.

[EIU and Arthur-Andersen(1995)] Economist Intelligence Unit EIU and Arthur-Andersen. *Managing Business Risks: An Integrated Approach*. Creating the future. Economist Intelligence Unit, 1995. URL https://books.google.de/books?id=SfEJAQAAMAAJ.

[ERNST&YOUNGS(2010)] ERNST&YOUNGS. Risk appetite: The strategic balancing act. 2010.

[ERNST&YOUNGS(2012)] ERNST&YOUNGS. Corporate governance:changing regulatory scenario and the role of thein dependent director. 2012.

[Forrester and Forrester(1971)] Jay Wright Forrester and Jay W Forrester. *World dynamics*. Wright-Allen Press Cambridge, MA, 1971.

[Frick et al.(2009)Frick, Servaes, Abts, Mehrtens, Söhnchen, Mülder, Stegemerten, and Westheide] D. Frick, I. Servaes, D. Abts, M. Mehrtens, P.G. Söhnchen, W. Mülder, B. Stegemerten, and J. Westheide. *Masterkurs Wirtschaftsinformatik: Kompakt, praxisnah, verständlich - 12 Lern- und Arbeitsmodule*. Vieweg Teubner Verlag, 2009. ISBN 9783834800022. URL https://books.google.at/books?id=BWba6yDzJrIC.

[FSA(2011)] Financial Services Authority FSA. Enhancing frameworks in the standardised approach to operational risk - guidance note, 2011.

[Gartner(2011)] Inc. Gartner. Magic quadrants and marketscopes: How gartner evaluates vendors within a market, 2011.

[Gerhard(2014)] Detlef Gerhard. Industrielle informationssysteme. Vorlesung 307.413 Industrielle Informationssysteme, 2014.

[Gigerenzer and Kober(2013)] G. Gigerenzer and H. Kober. *Risiko: Wie man die richtigen Entscheidungen trifft*. C. Bertelsmann Verlag, 2013. ISBN 9783641119904. URL https://books.google.de/books?id=0sGNJNkkPjYC.

[Gleissner(2011)] W. Gleissner. *Grundlagen des Risikomanagements im Unternehmen, Controlling, Unternehmensstrategie und wertorientiertes Management*. Vahlen, 2011.

[Gleissner and Mott(2008)] Werner Gleissner and Bernd Mott. Risikomanagement auf dem prüfstand. pages S. 53–63, Feb 2008.

[Gumm and Sommer(2013)] H.P. Gumm and M. Sommer. *Einführung in die Informatik*. De Gruyter, 2013. ISBN 9783486719956. URL https://books.google.at/books?id=eUHpBQAAQBAJ.

[Hillson(1997)] David A Hillson. Towards a risk maturity model. *The International Journal of Project and Business Risk Management*, 1(1):35–45, 1997.

[ICAEW(1997)] Institute of Chartered Accountants in England & Wales ICAEW. Financial reporting of risk. proposals for a statement of business risk. 1997.

[ICC(2013)] International Chamber of Commerce ICC. The icc antitrust compliance toolkit. Technical report, 2013.

[IPMA et al.(2006)] International Project Management Association IPMA et al. *ICB-IPMA competence baseline version 3.0*. 2006.

[ISACA(2012)] COBIT ISACA. 5: A business framework for the governance and management of enterprise it. *Rolling Meadows: ISACA*, 2012.

[ISO(2008)] Internationalen Organisation für Normung ISO. Iso iec 15288 systems and software engineering system life cycle processes, Jan 2008.

[ISO(2009)] Internationalen Organisation für Normung ISO. Din iso 31000 risikomanagement - grundsätze und leitlinien, 2009.

[Kahneman(2011)] D. Kahneman. *Thinking, Fast and Slow*. Farrar, Straus and Giroux, 2011. ISBN 9781429969352. URL `https://books.google.de/books?id=ZuKTvERuPG8C`.

[Kaplan and Mikes(06.2012)] Robert S. Kaplan and Anette Mikes. Managing risks - a new framework. 06.2012. URL `http://hbr.org/2012/06/managing-risks-a-new-framework/ar/`.

[Klinger and Klinger(2009)] Michael A. Klinger and Oskar Klinger. *Das interne Kontrollsystem im Unternehmen; Checklisten, Organisationsanweisungen, Praxisbeispiele und Muster-Prüfberichte*. Controlling competence. Vahlen, München, 2. aufl. edition, 2009. ISBN 978-3-8006-3656-3. 1. Aufl. u.d.T. Klinger, Michael A.: Das interne Kontrollsystem (IKS) im Unternehmen.

[KPMG and EIU(2013)] KPMG and Economist Intelligence Unit EIU. Expectations of risk management outpacing capabilities - it is time for action. 2013.

[Krcmar(2015)] Helmut Krcmar. *Einführung in das Informationsmanagement*. Springer-Lehrbuch. Springer Berlin Heidelberg, Berlin, Heidelberg, 2., überarb. aufl. 2015 edition, 2015. ISBN 978-3-662-44329-3.

[Leser and Naumann(2007)] U. Leser and F. Naumann. *Informationsintegration: Architekturen und Methoden zur Integration verteilter und heterogener Datenquellen*. dpunkt-Verlag, 2007. ISBN 9783898644006.

[Levy(März 2015)] Cindy Levy. Managing the people side of risk - risk culture transformation. März 2015.

[Löhr(2010)] Benjamin W. Löhr. *Integriertes Risikocontrolling für Industrieunternehmen; eine normative Konzeption im Kontext der empirischen Controllingforschung von 1990 bis 2009*. Controlling and business accounting ; 4. Lang, Frankfurt am Main ; Wien [u.a.], 2010. ISBN 978-3-631-61031-2. Zugl.: Giessen, Univ., Diss., 2010.

[Löw et al.(2010)Löw, Pabst, and Petry] Peter Löw, Roland Pabst, and Erwin Petry. *Funktionale Sicherheit in der Praxis; Anwendung von DIN EN 61508 und ISO/DIS 26262 bei der Entwicklung von Serienprodukten*. dpunkt, Heidelberg, 1. aufl. edition, 2010. ISBN 978-3-89864-570-6.

[Maissner(2010)] Bernadette Maissner. Risikomanagement und risikocontrolling in großen familienunternehmen, 2010. Linz, Univ., Dipl.-Arb., 2010.

[Marco and Lister(1987)] Tom de Marco and T. Lister. *Peopleware: Productive projects and teams.* New York (USA), Dorset House, 1987.

[MaRisk(2014)] Fachgremium MaRisk. Mindestanforderungen an das risikomanagement interpretationsleitfaden, version 5.1. Technical report, Deutscher Sparkassen- und Giroverband, 2014.

[McNeil et al.(2015)McNeil, Frey, and Embrechts] A.J. McNeil, R. Frey, and P. Embrechts. *Quantitative Risk Management: Concepts, Techniques and Tools*. Princeton Series in Finance. Princeton University Press, 2015. ISBN 9781400866281. URL `https://books.google.de/books?id=SfJnBgAAQBAJ`.

[McNish(März 2013)] Rob McNish. Getting to erm. (43), März 2013.

[Neuhauser(2011)] Mathias Neuhauser. It-gestütztes risikomanagement - ermittlung der anforderungen an ein analytisches informationssystem und konzeptioneller entwurf, 2011. Linz, Univ., Master-Arb., 2011.

[ÖCGK(2015)] Österreichischer Arbeitskreis Corporate Governance ÖCGK. Österreichischer corporate governance kodex, 2015.

[Oelkers and Bitzyk(2009)] Janine Oelkers and Peter. Bitzyk. Die neue regelpublizität nach börseg 2007 und uräg 2008. 2009.

[Olsen et al.(2011)Olsen, Plaschke, and Stelter] E. Olsen, F. Plaschke, and H. Stelter, D.and Farag. Value creation in a volatile economy - risky business. 2011.

[ONR(2014a)] Österreichisches Normungsinstitut ONR. Onr 49000 risikomanagement für organisation und systeme - begriffe und grundlagen - umsetzung von iso31000 in die praxis, 2014a.

[ONR(2014b)] Österreichisches Normungsinstitut ONR. Onr 49001 risikomanagement, 2014b.

[ONR(2014c)] Österreichisches Normungsinstitut ONR. Onr 49002-1 leitfaden für die einbettung des risikomanagement ins managementsystem, 2014c.

[ONR(2014d)] Österreichisches Normungsinstitut ONR. Onr 49002-2 methoden der risikobeurteilung, 2014d.

[OpRisk-Advisory and Towers-Perrin(2010)] OpRisk-Advisory and Towers-Perrin. A new approach for managing operational risk. revised, 2010.

[Pape(2011)] U. Pape. *Grundlagen der Finanzierung und Investition: Mit Fallbeispielen und Übungen*. De Gruyter, 2011. ISBN 9783486714555. URL `https://books.google.at/books?id=9nToBQAAQBAJ`.

[Pergler(Dezember 2012)] Martin Pergler. Whats different in the corporate world. (40), Dezember 2012.

[Pergler(Oktober 2013)] Martin Pergler. Strategic commodity and cash-flow-at-risk modeling for corporates. (51), Oktober 2013.

[Pichler(2002)] Mario Pichler. Risikomanagement in österreichs großunternehmen; teil 1 - grundlagen des risikomanagements, identifikation und bewertung von risiken sowie eine empirische studie zum entwicklungsstand in der unternehmenspraxis, 2002. Linz, Univ., Dipl.-Arb., 2002.

[Plaschke et al.(2013)Plaschke, Rodt, Pidun, and Günther] F. Plaschke, M. Rodt, U. Pidun, and F. Günther. The art of risk management. 2013.

[PMI(2014)] Project Management Institute PMI. *Project Management Body of Knowledge*. Fifth edition, 2014.

[Popescu(2014)] Alina Cristina Popescu. Risk management fundamentals. TU WIEN - Vorlesung IT-based Management am 23.10.2014, 2014.

[Power et al.(2013)Power, Ashby, and Palermo] Michael Power, S. Ashby, and T. Palermo. Risk culture in financial organisations. *London School of Economics, London*, 2013.

[Purgathofer(2006)] Peter Purgathofer. is informatics a design discipline? (volume 4):pp 303–314., december 2006.

[pwc(2008)] PricewaterhouseCoopers AG pwc. A practical guide to risk assessment. 2008.

[pwc(2011)] PricewaterhouseCoopers AG pwc. Risk management benchmarking 2011/12. 2011.

[Racz(2011)] Nicolas Racz. Governance, risk and compliance (grc) for information systems - towards an integrated approach, 2011. Wien, Techn. Univ., Diss., 2011.

[Radinger(2010)] Wolfgang Radinger. It vertiefung. Vorlesung 384.079 Informationstechnik, 2010.

[Raz and Hillson(2005)] Tzvi Raz and David Hillson. A comparative review of risk management standards. *Risk Management*, pages 53–66, 2005.

[Reiß and Reker(2011)] Herbert Reiß and Jürgen Reker. Compliance im mittelstand. 2011.

[RMA(2011)] Riskmanagement Association e.V. RMA. Grundsätze eines ordnungsmäßigen risikomanagements. Technical report, Riskmanagement Association e.V., 2011.

[Röhrenbacher(2008)] H. Röhrenbacher. *Finanzierung und Investition (mit Excel und HP): Finanzplanung mit Cash-flow-Statements ; alle Investitionsrechnungsverfahren ; ausführlich kommentierte Beispiele für Excel 2007 von Hans Röhrenbacher*. Fachbuch Wirtschaft. Linde, 2008. ISBN 9783714301489. URL `https://books.google.at/books?id=mFem2InH4ScC`.

[Romeike and Hager(2009a)] Frank Romeike and Peter Hager. *Erfolgsfaktor Risiko Management 2.0. Methoden, Beispiele, Checklisten ; Praxishandbuch für Industrie und Handel*. Gabler, Wiesbaden, 2., vollst. überarb. und erw. aufl. edition, 2009a. ISBN 978-3-8349-0895-7.

[Romeike and Hager(2009b)] Frank Romeike and Peter Hager. *Erfolgsfaktor Risiko Management 2.0. Methoden, Beispiele, Checklisten ; Praxishandbuch für Industrie und Handel*. Gabler, 2009b.

[Romeike and Hager(2013)] Frank Romeike and Peter Hager. *Erfolgsfaktor Risiko-Management 3.0; Methoden, Beispiele, Checklisten ; Praxishandbuch für Industrie und Handel*. Springer Gabler, Wiesbaden, 3. aufl. edition, 2013. ISBN 978-3-8349-3339-3; 3-8349-3339-2. 2. Aufl. u.d.T Romeike, Frank: Erfolgsfaktor Risiko-Management 2.0.

[Schafferer(2011)] Michael Schafferer. Vo 07: Organisatorische sicherheit/sicherheitsmanagement. Vorlesung 183.235 Internet Security, 2011.

[Scheer(2013)] A.W. Scheer. *ARIS - Vom Geschäftsprozeß zum Anwendungssystem*. Springer Berlin Heidelberg, 2013. ISBN 9783642978197.

[Scheld(2012)] Guido A. Scheld. *Controlling im Mittelstand. Band 2: Unternehmenscontrolling*. 2012. ISBN 3932647556.

[Schifferstein and Hekkert(2011)] H.N.J. Schifferstein and P. Hekkert. *Product Experience*. Elsevier Science, 2011. ISBN 9780080556789. URL `https://books.google.de/books?id=iQnfJHjcVQ8C`.

[Schleinzer(2014)] Andreas Schleinzer. Entwickung eines reifegradmodells für das unternehmensweite risikomanagement, 2014.

[Schwaiger(2013)] Walter Schwaiger. Enterprise risk management - fundamentals. Vorlesung 330.239, 2013.

[Schwarzer and Krcmar(2014)] Bettina Schwarzer and Helmut Krcmar. *Wirtschaftsinformatik*, volume 5. 2014.

[Shenkir and Walker(2007)] William G. Shenkir and Paul L. Walker. Enterprise risk management: Tools and techniques for effective implementation. 2007. URL `www.imanet.org`.

[Silbermayr(2012)] Stefanie Silbermayr. Bewertungsmethoden im risikomanagement, 2012. Linz, Univ., Dipl.-Arb., 2012.

[Simons(1999)] Robter Simons. How risky is your company? (77), Jan-Feb 1999.

[Sitterli(2012)] Christopher Heinz Sitterli. Risikomanagement börsennotierter unternehmen in österreich, 2012. Linz, Univ., Dipl.-Arb., 2012.

[Stegemann(Februar 2014)] Uwe Stegemann. Enterprise-risk-management practices: Where is the evidence? (53), Februar 2014.

[Sterman(2000)] John D Sterman. *Business dynamics: systems thinking and modeling for a complex world*, volume 19. Irwin/McGraw-Hill Boston, 2000.

[Taleb(2008)] N.N. Taleb. *The Black Swan: The Impact of the Highly Improbable*. Penguin Books Limited, 2008. ISBN 9780141906201. URL `https://books.google.de/books?id=Wu1MJmle10YC`.

[Taleb(2012)] N.N. Taleb. *Antifragile: Things that Gain from Disorder*. Penguin Books Limited, 2012. ISBN 9780718197902. URL `https://books.google.de/books?id=T9hbUv4NIU0C`.

[Vanini(2012)] Ute Vanini. *Risikomanagement: Grundlagen-Instrumente-Unternehmenspraxis*. Schäffer-Poeschel Verlag für Wirtschaft Steuern Recht GmbH, 2012.

[VDI(2005)] Fachbereich Sicherheit und Management VDI. Integrierte managementsysteme (ims) - handlungsanleitung zur praxisorientierten einführung - allgemeine aussagen, 2005.

[Vollmuth and Zwettler(2013)] J.H. Vollmuth and R. Zwettler. *Kennzahlen: TaschenGuide*. Haufe TaschenGuide. Haufe Lexware, 2013. ISBN 9783648038536. URL `https://books.google.at/books?id=c7hLlKWgZE0C`.

[Wagner and Patzak(2015)] K.W. Wagner and G. Patzak. *Performance Excellence - Der Praxisleitfaden zum effektiven Prozessmanagement*. Carl Hanser Verlag GmbH, 2015. ISBN 9783446431812.

[Wengert and Schittenhelm(2013)] H. Wengert and F.A. Schittenhelm. *Corporate Risk Management*. Springer Berlin Heidelberg, 2013. ISBN 9783642366895. URL `https://books.google.de/books?id=nDgiBAAAQBAJ`.