TECHNISCHE UNIVERSITÄT WIEN
Vienna University of Technology

DIPLOMARBEIT

Entwicklung eines Reifegradmodells für das unternehmensweite Risikomanagement

ausgeführt zum Zwecke der Erlangung des Akademischen Grades eines

Diplom-Ingenieurs

unter der Leitung von

Univ.Prof. Mag.rer.soc.oec. Dr.rer.soc.oec. Walter SCHWAIGER, MBA

Institut für Managementwissenschaften (E330)
Arbeitsbereich Finanzwirtschaft und Controlling

eingereicht an der Technischen Universität Wien

Fakultät für Maschinenwesen und Betriebswissenschaften

durch

Andreas Schleinzer

0271252 (E740)
Währinger Gürtel 95/11
A-1180 Wien

Wien, am 20. Juli 2014

Meiner Familie gewidmet.

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 20. Juli 2014 .....

(Andreas Schleinzer)

Danksagung

An dieser Stelle möchte ich mich bei allen Personen bedanken, die mich bei der Erstellung dieser Arbeit tatkräftigt unterstützt und immer wieder motiviert haben.

Zu Beginn möchte ich allen Mitarbeitern des Instituts für Managementwissenschaften – Fachbereich Finanzwirtschaft und Controlling an der Technischen Universität Wien unter der Leitung von Herrn Univ. Prof. Mag. Dr. Walter Schwaiger recht herzlich danken. Ich habe einen großen Teil meines Studiums an diesem Institut absolviert und konnte mich auf dem Gebiet des Risikomanagements bestens vertiefen.

Ein Besonderer Dank gilt Herrn Univ. Prof. Mag. Dr. Walter Schwaiger für die hervorragende Betreuung und Hilfestellung bei der Durchführung dieser Diplomarbeit. Es waren vor allem seine hilfreichen Anregungen, welche mir in zahlreichen Besprechungen immer neue Blickwinkel eröffneten und wesentlich zum Gelingen dieser Diplomarbeit beitrugen.

Das größte Dankeschön geht jedoch an meine Eltern, die mir mein Studium finanziell ermöglicht haben und mir immer Vertrauen, Verständnis und Unterstützung, aber auch den entsprechenden Freiraum zur Entfaltung entgegengebracht haben. Vielen Dank auch an Heidi, die meine Launen die ganze Zeit über mit viel Geduld ertragen hat und mir stets motivierend zur Seite stand.

Wien, am 20. Juli 2014 Andreas Schleinzer

Kurzfassung

Die Standortbestimmung vorhandener RM-Fähigkeiten stellt einen wesentlichen Schritt in der Verbesserung und Anwendung des Risikomanagements in Unternehmen dar. Das erste Reifegradmodell im Risikomanagement war das Risk Maturity Model (RMM) von David Hillson aus dem Jahr 1997. Darin werden 4 Reifegrade wachsender RM-Fähigkeiten beschrieben, namentlich „Naive“, „Novice“, „Normalised“ und „Natural“. Das Verständnis eines unternehmensweiten Risikomanagements im Sinne des COSO II-Rahmenwerks ist darin jedoch nicht Gegenstand der Betrachtung. Dabei wäre es für eine wertorientierte Unternehmensführung von großer Bedeutung, Synergiepotenziale jener RM-Funktionen im Unternehmen zu nutzen, welche in der einen oder anderen Weise mit für den Umgang mit Risiken verantwortlich sind.

Auf Basis des Capability Maturity Model Integration der Carnegie Mellon University wird ein Reifegradmodell für das unternehmensweite Risikomanagement (ERM) entwickelt, in dem alle wesentlichen RM-Funktionen eines Unternehmen berücksichtigt sind. Die Anwendung dieses ERM-Reifegradmodells ermöglicht Unternehmen somit die Beurteilung einzelner RM-Bereiche, wodurch Fehlerquellen gezielter aufgedeckt und entsprechende Verbesserungspotenziale abgeleitet werden können.

Abstract

An essential step in the improvement and application of risk management in companies is to define, if there are already existing risk management capabilities and how they are worked with. The first known maturity model in the field of risk management, the Risk Maturity Model (RMM), was invented by David Hillson in 1997. In this model Hillson describes four levels of maturity which are named „Naive“, „Novice“, „Normalised“ and „Natural“. The enterprise-wide risk management based on the COSO II framework is not part of this model. Although it would be of great importance for profit-oriented management to make use of synergetic potential of those areas in a company, where risk is worked with.

Based on the Capability Maturity Model Integration (CMMI), developed by the Carnegie Mellon University, an enterprise-wide risk maturity model (ERM) can be generated, where all different areas which are relevant for risk management are included. The application of this ERM-maturity model enables companies to evaluate individual risk management areas. With this approach it is easier to find sources of error and identify potentials of improvement.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Kapitel 1
Einleitung

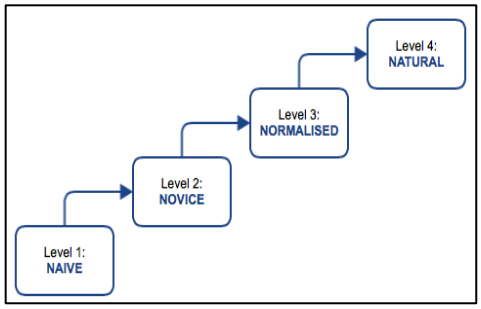
Motivation

Die Bedeutung des Risikomanagements (RM) ist in den letzten Jahren aufgrund der verschärften Wettbewerbssituation, den globalen Unsicherheiten sowie den Anforderungen von externen Stakeholdern stark gestiegen [Theuermann & Ebner 2012, S. 1]. Die jüngste Wirtschafts- und Finanzkrise hat verdeutlicht, dass die Fähigkeiten eines Unternehmens bei der Quantifizierung und der Bewältigung von Risiken noch deutlicher ausgebaut werden müssen. Ziel ist ein Risikomanagement als Instrument der Krisenabwehr und Pfeiler für eine wertorientierte Unternehmensführung [Vgl. Gleissner 2011, S. 1]. Die Standortbestimmung der vorhandenen RM-Fähigkeiten stellt einen wesentlichen Schritt in der Verbesserung und Anwendung des Risikomanagements in Unternehmen dar. Aus dem Benchmark lassen sich anschließend vorhandene Potentiale und Defizite erkennen und entsprechende Maßnahmen ableiten [Wiggert 2009, S. 136]. Um den Entwicklungsstand einer bestimmten Klasse von Objekten zu erheben, haben sich in der Literatur sogenannte Reifegradmodelle in verschiedenen Anwendungsdomänen etabliert. Zu den Meilensteinen der Forschung zählt sicherlich das 1991 an der Carnegie Mellon University entwickelte Capability Maturity Model (CMM), welches 2006 durch das Nachfolgermodell Capability Maturity Model Integration (CMMI) ersetzt wurde [Chrissis, Konrad & Shrum 2006, S. 6].

Problemstellung

Ein Standardwerk für Risikomanagement-Reifegradmodelle ist nach wie vor der Beitrag „Towards a Risk Maturity Model“ von David Hillson aus dem Jahre 1997, in dem der Autor die Idee des CMM aufgreift und daraus ein Modell mit vier Reifegraden (Abbildung 1) entwickelt. Auf der ersten Stufe (Naive) hat eine Organisation keinen strukturierten Umgang mit Unsicherheiten etabliert. Eine Organisation auf Stufe zwei (Novice) experimentiert mit der Anwendung des Risikomanagements. Die dritte Stufe (Normalised) beschreibt eine Organisation, die das Risikomanagement routinemäßig und strukturiert in fast allen Bereichen einsetzt.

Auf der letzten Stufe (Natural) ist das Risikomanagement integraler Bestandteil der Organisationskultur und kommt damit in allen Aspekten der Organisation proaktiv zur Anwendung [Vgl. Hillson 1997, S. 35].



	Level 1: NAIVE	Level 2: NOVICE	Level 3: NORMALISED	Level 4: NATURAL
KULTUR	Notwendigkeit von RM nicht bewusst	potentieller Nutzen des RM kaum bewusst	akzeptierte Strategie des RM	RM-Kultur
PROZESS	kein formaler Prozess	kein strukturierter Prozess	allgemeine Prozesse auf die meisten Projekte angewandt	RM-Informationen werden aktiv genutzt
ERFAHRUNG	keine Kenntnisse der Risikoprinzipien	erste Experimente im RM	ausgebildete interne Mitarbeiter	RM wird in allen Bereichen angewandt
ANWENDUNG	kein strukturiertes Vorgehen für das Managen von Unsicherheiten	RM-Anwendungen haben keine Beständigkeit	RM ist Bestandteil des Tagesgeschäfts	Risiko-basierte Berichterstattung und Entscheidungs-findung

Abbildung 1: RMM nach Hillson [Vgl. Hillson 1997, S. 35]

Hillson bezog sich bei der Entwicklung des RMM auf das damalig aktuelle CMM der Carnegie Mellon University. Dieses wurde jedoch weiterentwickelt und durch das Nachfolgermodell CMMI abgelöst, welches sich von seinem Vorgänger vor allem dadurch unterscheidet, dass es eine organisationweite Bewertung und Verbesserung der Geschäftsprozesse anstrebt [CMMI Product Team 2011, S. 18]. Ein CMMI-konformes Risikomanagement-Reifegradmodell würde die Vorteile dieser Weiterentwicklung aufgreifen und somit einen bedeutenden Mehrwert darstellen.

Eine weitere Schwachstelle des RMM stellt das fehlende Verständnis eines unternehmensweiten Risikomanagements (ERM) dar. Hillson fordert auf Reifegrad 3 (Normalised) zwar den strukturierten Einsatz des Risikomanagements in allen Bereichen, geht jedoch nicht auf die Definition eines unternehmensweiten Risikomanagements ein. Dabei würde gerade die unternehmensweite Definition des Risikomanagements nach COSO II die Möglichkeit bieten, risikorelevanten Funktionen im Unternehmen aufzuzeigen, abzugrenzen und Synergiepotenziale aufzuzeigen.

Zur Bestimmung der Reifegrade legt Hillson auf jeder Stufe bestimmte Kriterien für vier Attribute (Kultur, Prozess, Erfahrung und Anwendung) fest. Diese Kriterien sind jedoch vorwiegend generischer Natur und werden für die einzelnen risikorelevanten Funktionen im Unternehmen nicht konkretisiert.

Erwartetes Resultat

Das erwartete Resultat der vorliegenden Arbeit ist ein Reifegradmodell für ein unternehmensweites Risikomanagement (ERM), in dem alle RM-Funktionen eines Unternehmens berücksichtigt werden. Dabei soll das 3 Lines of Defense Model (3LoD-Modell) als Referenzmodell dienen, um die verschiedenen RM-Funktionen im Unternehmen voneinander abzugrenzen und vorhandene Synergiepotenziale aufzuzeigen. Entsprechend der COSO II Zieldimensionen wird anschließend eine Risikokategorisierung vorgenommen. Diese Kategorisierung verdeutlicht, welche Risiken im Unternehmen vorhanden sind und wo sie im 3LoD-Model adressiert werden. Basierend auf den Reifegraden des CMMI werden durch Heranziehen der ISO 31000-Inhalte die einzelnen ISO 31000-Reifegrad-Kriterien formuliert und ERM-Reifegrad-Kriterien abgeleitet. Durch diese CMMI-konforme Darstellung des ISO 31000-Standards werden die CMMI-Reifegrade um den Risikoaspekt erweitert. Abschließend sollen die ERM-Kriterien für die einzelnen Säulen im 3LoD-Modell konkretisiert und zum unternehmensweiten Reifegradmodell zusammengefasst werden.

Verwendete Methoden

- Capability Maturity Model Integration – CMMI
- COSO II-Rahmenwerk
- ISO 31000
- Three Lines of Defense Model – 3LoD Model

Kapitel 2

Theoretische Grundlagen zu Reifegradmodellen

2.1 Grundlagen zu Reifegradmodellen

Seit der Einführung des Capability Maturity Models durch das Software Engineering Institute der Carnegie Mellon University im Jahr 1991 haben sich Reifegrad-Modelle in den verschiedensten Anwendungsdomänen etabliert [Vgl. Wendler 2012, S. 1317]. Die Ursprünge derartiger Stufenmodelle lassen sich in vorausgegangen Arbeiten von Maslow und Crosby identifizieren [Schierenbeck 2003, S. 58]. Als Vorreiter entwickelte der Psychologe Maslow ein Stufenmodell, das eine Hierarchie menschlicher Bedürfnisse darstellt und im deutschen Sprachraum auch als Maslowsche Bedürfnispyramide bezeichnet wird. Crosby beschäftigte sich im Zuge seiner Forschung intensiv mit dem Thema Qualitätsmanagement und entwickelte im Jahr 1979 das Quality Management Maturity Grid (QMMG), wobei er bei dessen Stufenfestlegungen mutmaßlich auf die Hierarchie von Maslow zurückgriff [Crosby 2000, S. 58].

2.1.1 Komponenten

Ungeachtet der unterschiedlichen Herangehensweisen an die Gestaltung von Reifegradmodellen, sollten jedoch laut De Bruin und Fraser alle diese Modelle folgende Bestandteile aufweisen [Vgl. Fraser et al. 2002, S. 246; De Bruin et al. 2005, S. 4]:

- eine Anzahl an Reifegradstufen mit treffender Bezeichnung,
- eine Anzahl an Dimensionen und Elementen bzw. Aktivitäten, welche diese einzelnen Dimensionen beschreiben und
- eine Zusammenfassung der Eigenschaften, die jeden Reifegrad charakterisieren bzw. eine generische Beschreibung der Aktivitäten je Reifegrad.

Reifegradstufen sind archetypische Reifegrade einer Dimension oder Domäne. Jede Reifegradstufe sollte eine klare Beschreibung ihrer Zielsetzung und ihrer Eigenschaften besitzen [Fraser et al. 2002, S. 246]. Typischerweise definieren Reifegradmodelle zwischen drei und sechs Reifegradstufen. Diese beschreiben Stationen auf einem antizipierten, logischen, gewünschten oder typischen Entwicklungspfad von einem Anfangsstadium bis zur vollkommenen Reife. Dabei bezeichnet die Reife einer Sache das Ausmaß, in dem eine vordefinierte Anforderung bezüglich des Entwicklungsstands erreicht wird [Mettler 2009, S. 337]. Reifegradstufen haben gemäß ihrer Rangfolge eine alphanumerische oder eine sprechende Bezeichnung, um die Semantik der einzelnen Entwicklungsstufen zum Ausdruck zu bringen [Kübel 2013, S. 59].

Reifegradmodelle sind meist multi-dimensional und beschreiben viele Merkmale der betrachteten Objekte [Kübel 2013, S. 59]. Dimensionen umfassen spezifische Fähigkeiten, Prozessbereiche und andere Gestaltungsobjekte, um einen Interessenbereich zu strukturieren. Dimensionen sollten vollständig und gut voneinander abgrenzbar sein. Sie werden entweder anhand von Bewertungselementen bzw. Messkriterien (Praktiken und Aktivitäten) oder qualitativen Beschreibungen spezifiziert [De Bruin et al. 2005, S. 5]. Die für ein Objekt festgestellten Reifegrade können von Dimension zu Dimension variieren, wodurch sich eine differenzierte Darstellung des Reifegrad-Profils ergibt [Kübel 2013, S. 59].

Ein Reifegrad ist durch festgelegte Merkmale des zu untersuchenden Objekts und durch die jeweils zur Erreichung des Reifegrads erforderlichen Merkmalsausprägungen definiert [Becker et al. 2009, S. 249]. Dabei kann ein höherer Reifegrad nur dann erreicht werden, wenn sowohl die Anforderungen der vorherigen als auch der angestrebten Stufe erfüllt sind. Die einzelnen Reifegrade geben dadurch Hilfestellungen, wann welche Verbesserungsmaßnahmen durchzuführen sind [Wendler 2012, S. 1318].

Die Ausgestaltung der oben aufgelisteten Bestandteile eines jeden Reifegradmodells erfolgt in der Praxis auf unterschiedliche Weise. Ausgehend von der Struktur lassen sich jedoch drei Typen von Reifegradmodelle in der Literatur unterscheiden [Vgl. Fraser et al. 2002, S. 246; Mettler 2010, S. 44]:

- **Rasterbasierte Modelle** sind einfache textuelle Beschreibungen der Reife eines Gestaltungsbereiches. Diese Modelle verwenden die gleiche Anzahl von Reifegradstufen und realitätsnahen Beschreibungen für alle Dimensionen und können daher als Tabelle oder Raster dargestellt werden. Die Reifebewertung wird anhand dieses Rasters vorgenommen.

- **Formal-strukturierte Modelle** nutzen Fragenkomplexe mit unterschiedlichen Fragetypen bzw. Bewertungsskalen. Jeder Reifegrad ist durch Regeln spezifiziert, welche zu erfüllen sind, um eine entsprechende Einstufung zu erreichen. Diese Modelle besitzen eine formale Struktur, welche durch ein Metamodell beschrieben wird.
- **Hybride Reifegradmodelle** gehen über rein textuelle Beschreibungen hinaus, nutzen aber nur relativ einfache Fragenkomplexe.

Neben der Erhebung des Entwicklungsstandes und der Identifikation von Verbesserungspotential versuchen Reifegradmodelle, einen Beitrag zur Bestimmung der Richtung bzw. des Ausmaßes von Entwicklungspotentialen in bestimmten Unternehmensbereichen zu leisten [Röglinger & Kamprath 2012, S. 510]. Das Fortschreiten auf einem Entwicklungspfad bedeutet eine stete Steigerung der Leistungsfähigkeit bzw. Güte der betrachteten Klasse von Objekten, wobei das Reifegradmodell als Skala zur Beurteilung dient. Wendler betont in diesem Zusammenhang die Bedeutung der evolutionären Verbesserung, sodass Anpassungen inkrementell vorgenommen werden können [Wendler 2012, S. 1319].

Die Anwendung von Reifegradmodellen zur Ermittlung der individuellen Reife des entsprechenden Anwendungsgebietes erfolgt i. d. R. mittels vorgegebener Bewertungsmethoden. Somit werden zu einem bestimmten Zeitpunkt Beobachtungen gesammelt und anschließend bewertet, um eine Zustandsaufnahme des betrachteten Objekts zu erhalten. Ausgehend von der ermittelten Ist-Situation lassen sich dadurch Verbesserungsvorschläge bzw. Handlungsempfehlungen ableiten [Vgl. Becker et al. 2009, S.250]. Bewertungsinstrumente können qualitativ oder quantitativ sein, so kommen in der Praxis vorwiegend Likert-Skalen[1]-gestaltete Fragebögen oder Scoring-Modelle[2] zum Einsatz [Vgl. Fraser 2002, S. 246].

2.1.2 Nutzen und Schwachstellen

Durch den Einsatz von Reifegradmodellen versprechen sich Unternehmen eine Reihe von Nutzenaspekten, bedenken jedoch oftmals nicht die damit verbundenen Schwachstellen bzw. Limitationen solcher Modelle. Im Folgendem werden die wesentlichen Vorteile und Nachteile, die mit dem Einsatz von Reifegradmodellen als Diagnoseinstrument verbunden sind, aufgelistet.

[1] Die Likert-Skala ist ein von Rensis Likert im Jahr 1932 entwickeltes Instrument der Einstellungsmessung. Es ist ein leistungsfähiges eindimensionales, personenorientiertes Skalierungsverfahren, welches auf Ratingskalen aufbaut. Durch summierte Einschätzungen soll die Einstellung einer Person als ablehnende oder zustimmende Haltung zum Einstellungsobjekt gefunden werden [Siehe http://de.wikipedia.org/wiki/Nutzwertanalyse].

[2] Beim Scoring-Modell (auch Nutzwertanalyse genannt) wird die Menge komplexer Handlungsalternativen analysiert, um Elemente dieser Menge entsprechend den Präferenzen des Entscheidungsträgers bezüglich eines multidimensionalen Zielsystems zu ordnen. Die Abbildung der Ordnung erfolgt durch die Angabe der Nutzwerte der Alternativen [Siehe http://de.wikipedia.org/wiki/Nutzwertanalyse].

Vorteile

- Reifegradmodelle stellen ein systematisches und hinsichtlich ihrer Dimensionen vollständiges Vorgehen bei der Identifizierung von Verbesserungsbereichen sicher.
- Aufgrund der einheitlichen Bewertung ermöglicht der Einsatz von Reifegradmodellen den Vergleich von Mitbewerbern am Markt. Auf Grundlage dieses Benchmarkings können dann entsprechende Wettbewerbsvorteile der Unternehmen gegenüber anderen gewonnen werden.
- Reifegradmodelle sind in gleichem Maße generisch und flexibel: Sie sind als Referenzmodell in sehr unterschiedlichen Organisationen anwendbar und mit Hilfe von Reifegrad-Assessments kann die spezifische Situation abgebildet und analysiert werden.
- Reifegrad-Assessments können schnell und unkompliziert durchgeführt werden und ermöglichen unmittelbares Feedback an die Teilnehmer. Ergebnisse können graphisch aufbereitet werden, wodurch eine schnelle Interpretation der Ergebnisse erleichtert wird.
- Ein Reifegradmodell unterstützt individuelles und organisationales Lernen, da es einen guten Überblick über Struktur, Praxis und Erfolgsfaktoren der jeweiligen Domäne gibt.
- Ein bedeutender Nutzenaspekt beim Einsatz von Reifegradmodellen bietet sich Unternehmen bei der Erfüllung interner und externer Normen bzw. gesetzlicher Auflagen.

Nachteile

- Im Rahmen eines Reifegrad-Assessment können zwar Anforderungen für eine Soll-Organisation festgelegt werden, jedoch spezifizieren Reifegradmodelle meist nicht explizit, welche Maßnahmen der Organisationsentwicklung erforderlich sind.
- Entscheidungsträger glauben sich in falscher Sicherheit, wenn ihre Entscheidungen ausschließlich auf Erkenntnissen aus Reifegradmodellen basieren. Reifegradmodelle haben blinde Flecken oder neigen zu einer Überbetonung von harten Fakten, da sie nur beobachtbare und abgrenzbare, nicht aber individuelle Fähigkeiten erfassen können.

- Es besteht die Gefahr, dass Modelle übersimplifizieren und wichtige Informationen vorenthalten, wodurch unzulässige Schlüsse gezogen werden können. Auch komplexe Modelle sind schwierig zu nutzen und führen bei falscher Anwendung ebenfalls zu irreführenden Ergebnissen. Ziel ist die Balance zwischen Komplexreduktion und Modelltreue.
- Reifegradmodelle geben in der Regel nur einen Entwicklungspfad vor, wobei weitere mögliche Pfade oft vernachlässigt werden.
- Eine bedeutende Schwachstelle von Reifegradmodellen zeigt sich in der Forderung, dass alle Anforderungen einer Reifegradstufe erfüllt sein müssen, unabhängig davon ob sie für das Unternehmen ökonomisch sind oder nicht.

2.2 Capability Maturity Model Integration – CMMI

CMMI hat seinen Ursprung im Software Capability Model (CMM) und wurde in den 1980er Jahren auf Initiative des US-Verteidigungsministeriums vom Software Engineering Institute (SEI) der Carnegie Mellon University entwickelt. Anfänglich als Methoden- und Werkzeugsammlung gedacht, war es das Ziel dieses Modells, die Effizienz von Entwicklungsprozessen im Software-Bereich zu bewerten und strukturiert zu verbessern [Vgl. Gausemeier & Plass 2014, S. 317]. CMMs sollen im Allgemeinen eine Verbesserung der Arbeitsabläufe innerhalb einer Organisation bewirken. Sie umfassen die wesentlichen Elemente wirksamer Arbeitsabläufe eines oder mehrerer Fachgebiete und beschreiben einen evolutionären Verbesserungsweg von unreifen Ad-Hoc-Arbeitsabläufen hin zu reifen und disziplinierten Prozessen mit verbesserter Qualität und Wirksamkeit [Vgl. CMMI Product Team 2011, S. 17].

2.2.1 Struktur und Aufbau

Im Laufe der Zeit folgten verschiedene Abwandlungen des CMM für eine Vielzahl von Disziplinen. Um dem Wildwuchs an vorhandenen Modellen entgegenzuwirken wurde im Jahr 2000 das Capability Maturity Model Integration (CMMI) mit dem Ziel veröffentlicht, ein einheitliches, modulares und vor allem allgemein verwendbares Modell zu erstellen [Vgl. Gausemeier & Plass 2014, S. 317]. Die Zusammenführung ausgewählter Modelle in einem einzelnen CMMI-Framework war darauf ausgerichtet, eine organisationsweite Bewertung und Verbesserung von Geschäftsprozessen zu ermöglichen. Zur Zeit der Veröffentlichung der ersten Version wurden zwei weitere CMMI-Modelle geplant und damit das Konzept der Konstellationen geboren [CMMI Product Team 2011, S. 18].

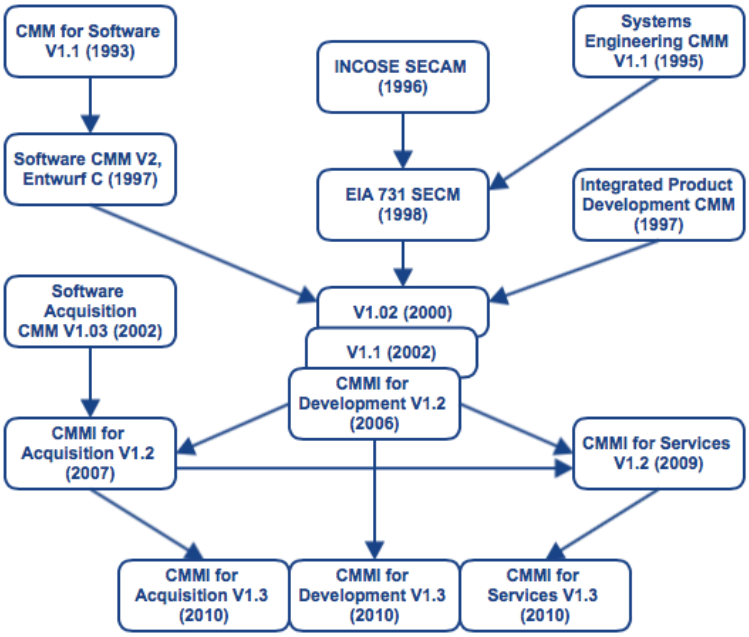


Abbildung 2: Geschichte des CMMI [CMMI Product Team 2011, S. 18]

Abbildung 2 zeigt die Geschichte des Reifegradmodells der Carnegie Mellon University, beginnend bei dessen Einführung im Jahr 1993 bis hin zur weiterentwickelten Version 1.3 im Jahr 2010, in der aktuell folgende drei Derivate unterschieden werden [Vgl. Gausemeier & Plass 2014, S. 317]:

- **CMMI-DEV** (CMMI for Development) dient der Beurteilung und Verbesserung der Effizienz von Produktentwicklungsprozessen.
- **CMMI-ACQ** (CMMI for Acquisition) adressiert die Leistungsbewertung und -steigerung von Organisationen, die im großen Umfang Systeme, Hardware oder Software zukaufen. Der Fokus liegt jedoch auf der Optimierung des Beschaffungsprozesses.
- **CMMI-SVC** (CMMI for Service) eignet sich vor allem für Organisationen, deren Kerngeschäft Dienstleistungen sind. Im Vordergrund stehen die Entwicklung und Bereitstellung sowie das Management von Dienstleistungen.

Alle angeführten CMMI-Modelle sind in ihrer grundlegenden Struktur identisch und werden aus dem CMMI-Framework erstellt. Wie in Abbildung 2 dargestellt, enthalten alle der drei Modelle die gleichen 16 Kernprozessgebiete, welche grundlegende Konzepte abdecken, die fundamental für jeden der drei Interessensgebiete sind (also Beschaffung, Entwicklung und Dienstleistung). Ein Teil des Materials der Kernprozessgebiete ist bei allen Konstellationen gleich, anderes Material kann an das jeweilige Interessensgebiet angepasst sein.

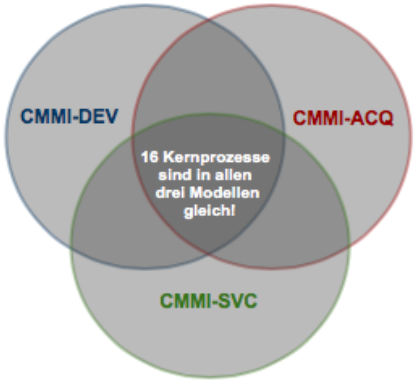


Abbildung 3: Kernprozesse aller CMMIs [Vgl. CMMI Product Team 2011, S. 21]

Grundsätzlich gehen alle der drei CMMI-Derivate von einer Reihe fest definierter Prozessgebiete aus. Am Beispiel des CMMI-DEV wird im Folgenden der Aufbau von CMMI erläutert. CMMI-DEV unterscheidet 22 Prozessgebiete, welche thematisch in vier Kategorien unterteilt werden (Abbildung 4). Ein Prozessgebiet besteht aus einer Reihe von Zielen und Praktiken und fasst alle Anforderungen zu einem bestimmten Thema zusammen.

Prozessmanagement	Projektmanagement
• Organisationsweite Prozessdefinition • Organisationsweite Prozessfähigkeit • Organisationsweites • Prozessmanagement • Organisationsweiter Prozessfokus • Organisationsweites Training	• Anforderungsmanagement • Integriertes Projektmanagement • Management von Lieferantenvereinbarungen • Projektverfolgung & -steuerung • Projektplanung • Quantitatives Projektmanagement • Risikomanagement
Ingenieurdisziplin	**Unterstützung**
• Anforderungsentwicklung • Produktintegration • Technische Umsetzung • Validierung • Verifizierung	• Entscheidungsanalyse & -findung • Konfigurationsmanagement • Messung & Analyse • Qualitätssicherung von Prozessen & Produkten • Ursachenanalyse & Problemlösung

Abbildung 4: Prozessgebiete des CMMI-DEV [Vgl. CMMI Product Team 2011, S. 21]

Es werden spezifische und generische Ziele und Praktiken unterschieden:

- **Spezifische Ziele:** Jedem Prozessgebiet sind mehrere spezifische Ziele zugeordnet, welche die eindeutigen Merkmale beschreiben, die vorhanden sein müssen, um ein Prozessgebiet zu erfüllen. Somit entsprechen die spezifischen Ziele den inhaltlichen Aufgaben des Prozessgebietes und sind Indikatoren für dessen Leistungsfähigkeit [Vgl. Gausemeier & Plass 2014, S. 317; CMMI Product Team 2011, S. 24].
- **Generische Ziele** beschreiben den Grad der Institutionalisierung[3] eines Prozessgebietes, also inwieweit spezifischen Ziele regelmäßig, dauerhaft und effizient umgesetzt werden. Diese Ziele sind übergreifend für alle Prozessgebiete formuliert und werden daher als generisch bezeichnet. Der Grad der Institutionalisierung ist jeweils in den generischen Zielen enthalten und kommt außerdem in den Namen der Prozesse zum Ausdruck, die mit den einzelnen Zielen verbunden sind [CMMI Product Team 2011, S. 80].

Definierte **Praktiken** der Prozessgebiete stellen, sowohl auf generischer als auch auf spezifischer Ebene, bewährte Methoden und Aktivitäten zur Verfügung und unterstützen dadurch die Organisation beim Erreichen der entsprechenden Ziele, sowie beim Realisieren und Verbessern der Prozessgebiete [CMMI Product Team 2011, S. 25].

2.2.2 Unterschiedliche Darstellung in Fähigkeits- und Reifegraden

CMMI ermöglicht zwei unterschiedliche Herangehensweisen zur Leistungsbewertung:

- eine kontinuierliche Bewertung anhand von Fähigkeitsgraden und
- eine stufenweise Bewertung mit Hilfe von Reifegraden.

Fähigkeitsgrade beziehen sich darauf, wie gut eine Organisation Prozessverbesserungen in einzelnen Prozessgebieten erreicht. Diese Grade dienen zur inkrementellen Verbesserung der Prozesse in einem gegebenen Prozessgebiet. **Reifegrade** beziehen sich darauf, wie gut eine Organisation Prozessverbesserungen auf mehreren Prozessgebieten erreicht. Diese Grade dienen dazu, die Prozesse zu verbessern, die zu einer gegebenen Menge von Prozessgebieten gehören [Vgl. Schrum et al. 2006, S 35]. Für die Reifegrade 2 bis 3 werden dieselben Bezeichnungen verwendet wie für die entsprechenden Fähigkeitsgrade. Diese einheitliche Terminologie ist beabsichtigt, da die Konzepte der Reife- und Fähigkeitsgrade einander ergänzen.

[3] Institutionalisieren bezeichnet hierbei das Etablieren von Vorgehensweisen in der Organisation, so dass die eingeführten Prozessabläufe von allen Beteiligten als selbstverständlich angesehen und umgesetzt werden [CMMI 2011].

Reifegrade charakterisieren die Verbesserungen einer Organisation bezogen auf einen Satz von Prozessgebieten, Fähigkeitsgrade die Verbesserung bezogen auf ein einzelnes Prozessgebiet [CMMI Product Team 2011, S. 35].

Grad	Darstellung in Fähigkeitsgraden	Darstellung in Reifegraden
0	Unvollständig	-
1	Durchgeführt	Initial
2	Geführt	Geführt
3	Definiert	Definiert
4	-	Quantitativ geführt
5	-	Prozessoptimierung

Tabelle 1: Gegenüberstellung von Fähigkeits- und Reifegrade im CMMI [CMMI Product Team 2011, S. 35]

Bei der **kontinuierlichen Bewertung** wird jedes Prozessgebiet getrennt betrachtet und anhand eines Fähigkeitsgrades von 0 bis 4 bewertet. Diese Art der Darstellung wird vorwiegend verwendet, wenn die zu verbessernden Prozessgebiete bekannt bzw. ineffiziente Prozessgebiete bereits identifiziert sind. Für den Übergang von einem Fähigkeitsgrad zum nächsten ist vor allem die Institutionalisierung der Prozesse erforderlich [Gausemeier & Plass 2014, S. 319]. Der Fortschritt dieser Prozessinstitutionalisierung wird mit Hilfe der generischen Ziele 1-3 und den Beschreibungen der einzelnen Prozessfortschritte charakterisiert:

	Prozessfortschritt
GZ 1	**Durchgeführter Prozess:** Ein durchgeführter Prozess ist ein Arbeitsablauf, der dafür sorgt, dass die zur Erfüllung der spezifischen Ziele eines Prozessgebiets erforderliche Arbeit verrichtet wird.
GZ 2	**Geführter Prozess:** Ein Prozess gilt als „geführt“, wenn er das Ziel „Durchgeführter Prozess“ erreicht und zusätzlich geplant wird.
GZ 3	**Definierter Prozess:** Ein Prozess gilt als „definiert“, wenn er das Ziel „Geführter Prozess“ erreicht und zusätzlich auf unternehmensweit standardisierte Prozesse zugeschnitten ist. Zudem soll er durch gesammelte Erfahrungen stets besser werden.

Tabelle 2: Generische Ziele und Prozessfortschritte im CMMI [Vgl. CMMI Product Team 2011, S. 80]

Ein Fähigkeitsgrad für ein Prozessgebiet ist erreicht, wenn alle generischen Ziele bis zu diesem Grad erfüllt sind. Für die Fähigkeitsgrade 2 und 3 werden dieselben Bezeichnungen verwendet wie für die generischen Ziele 2 und 3. Dies ist beabsichtigt, denn durch die Umsetzung der generischen Ziele und Praktiken werden die entsprechenden Fähigkeitsgrade erreicht.

- **Fähigkeitsgrad 0 – unvollständig:** Ein oder mehrere spezifische Ziele des Prozessgebietes werden nicht erreicht.
- **Fähigkeitsgrad 1 – durchgeführt:** Alle spezifischen Ziele des Prozessgebietes sind erfüllt, somit ist das generische Ziel „durchgeführter Prozess" erreicht. Verbesserungen können jedoch mit der Zeit verloren gehen, da sie nicht institutionalisiert sind.
- **Fähigkeitsgrad 2 – geführt:** Ein Prozess auf Fähigkeitsgrad 2 wird als „geführt" bezeichnet.
- **Fähigkeitsgrad 3 – definiert:** Ein Prozess auf Fähigkeitsgrad 2 wird als „definiert" bezeichnet.

Bei der **stufenweisen Darstellung** wird das gesamte Unternehmen mit einem Reifegrad bewertet. Die Fähigkeitsgrade der einzelnen Prozessgebiete werden nicht explizit genannt. Dieser Ansatz wird verwendet, wenn eine Verbesserung aller Prozessgebiete angestrebt wird. Grundlage der stufenweisen Darstellung ist eine Hierarchisierung der Prozessgebiete, wie in Tabelle 1 ersichtlich. Diese Hierarchisierung beruht auf den Interdependenzen zwischen den einzelnen Prozessgebieten und legt fest, in welcher Reihenfolge diese verbessert werden sollen [Vgl. CMMI Product Team 2011, S. 80].

Bei der Darstellung in Reifegraden sind die Prozessgebiete nach Reifegraden gruppiert, um anzuzeigen, welche Prozessgebiete umgesetzt werden müssen, damit eine Organisation einen bestimmten Reifegrad erreicht. Tabelle 3 zeigt auch die Möglichkeit der äquivalenten Einstufung, bei der eine Organisation, welche eine Darstellung in Fähigkeitsgraden verwendet, ihr Fähigkeitsgradprofil in die entsprechende Reifegradbewertung umwandeln kann. Dabei stehen die schattiert hinterlegten Bereiche in der Spalte der Fähigkeitsgrade für die Zielprofile, die dem jeweiligen Reifegrad entsprechen [Vgl. Schrum et al. 2006, S 57].

Prozessgebiet	Reifegrad	FG 1	FG 2	FG 3
Anforderungsmanagement	2	Zielprofil 2		
Konfigurationsmanagement	2			
Management von Lieferantenvereinbarungen	2			
Messung und Analyse	2			
Projektplanung	2			
Projektverfolgung und -steuerung	2			
Qualitätssicherung von Prozessen und Produktion	2			
Anforderungsentwicklung	3	Zielprofil 3		
Entscheidungsanalyse und -findung	3			
Integriertes Projektmanagement	3			
Organisationsweite Prozessdefinition	3			
Organisationsweiter Prozessfokus	3			
Organisationsweites Training	3			
Produktintegration	3			
Risikomanagement	3			
Technische Umsetzung	3			
Validierung	3			
Verifizierung	3			
Organisationsweite Prozessfähigkeit	4	Zielprofil 4		
Quantitatives Projektmanagement	4			
Organisationsweites Prozessfähigkeitsmanagement	5	Zielprofil 5		
Ursachenanalyse und Problemlösung	5			

Tabelle 3: Prozessgebiete in CMMI [Vgl. CMMI Product Team 2011, S. 80]

Zur Erreichung eines höheren Reifegrades müssen die Anforderungen aller vorherigen Stufen vollständig erfüllt sein [CMMI Product Team 2011, S. 39]:

Reifegrad 1 – Initial: In Unternehmen mit Reifegrad 1 werden Arbeitsabläufe für gewöhnlich ad hoc und chaotisch durchgeführt. Es wird im Allgemeinen keine stabile Umgebung zur Unterstützung dieser Arbeitsläufe bereitgestellt. Die notwendigen Arbeiten werden zwar verrichtet, die Leistung hängt jedoch größtenteils von der Motivation und Kompetenz der Mitarbeiter ab. Dadurch werden oft wichtige Arbeitsabläufe vernachlässigt. Zufällige Erfolge können aufgrund der fehlenden Institutionalisierung der Arbeitsabläufe nicht wiederholt werden. Grundsätzlich erreicht jedes Unternehmen mindestens diesen Reifegrad.

Reifegrad 2 – Geführt: Arbeitsabläufe haben eine grundlegende Infrastruktur zu deren Umsetzung und werden in Einklang mit den unternehmensweiten Leitlinien geplant und ausgeführt. Zusätzlich werden diese Arbeitsabläufe überwacht, gesteuert und geprüft. Fachleute werden mit entsprechenden Ressourcen eingesetzt, um kontrollierte Ergebnisse zu erzielen. Verpflichtungen gegenüber relevanten Stakeholdern werden etabliert und nach Bedarf überarbeitet. Es gibt erste Anforderungen an Ergebnisse durch das Unternehmen und bei Abweichungen der tatsächlichen von den geplanten Ergebnissen werden entsprechende Korrekturmaßnahmen ergriffen. Arbeitsabläufe werden gemäß dokumentierter Praktiken durchgeführt und gelenkt, wodurch bestehende Verfahren auch unter Belastung beibehalten werden können. Außerdem ist der Zustand der Arbeitsergebnisse für das Management an definierten Punkten sichtbar.

Reifegrad 3 – Definiert: Mittlerweile sind Arbeitsabläufe gut charakterisiert und verstanden und werden in Form von Normen, Verfahren, Hilfsmitteln und Methoden beschrieben. Es existiert ein organisationsspezifischer Satz von Standardprozessen[4], aus dem der definierte Prozess durch Tailoring[5] ausgestaltet werden kann. Demnach werden Standards, Prozessbeschreibungen und Prozeduren passend für Projekte oder Organisationseinheiten abgeleitet. Auf Reifegrad 3 verbessert die Organisation die Prozesse weiter, die zu den Prozessgebieten von Reifegrad 2 gehören. Die im Reifegrad 2 noch nicht angegangenen generischen Praktiken des generischen Ziels 3 werden jetzt angewendet.

Reifegrad 4 – Quantitativ geführt: Beim Reifegrad 4 werden quantitative Ziele für die Qualitäts- und Prozessleistung etabliert und als Kriterien für das Management von Projekten verwendet. Diese quantitativen Ziele basieren auf den Bedürfnissen der Kunden, der Endanwender, der Organisation und der Prozessbeteiligten. Wesentlich ist, dass vorerst nur Teilprozesse mit dem größten Gesamtwert für das Unternehmen ausgewählt und mit Kennzahlen überwacht werden. Für diese Auswahl ist es entscheidend, die Beziehungen zwischen den Teilprozessen und ihre Auswirkung auf das Erreichen der Unternehmensziele zu verstehen. Außerdem unterstützen statistische und andere quantitative Methoden die Auswertung von Kennzahlen und erlauben Leistungsprognosen der ausgewählten Teilprozesse. Vorhersagen gründen sich teilweise auf einer statistischen Analyse detaillierter Prozessdaten. Bei Reifegrad 4 liegt der Schwerpunkt darauf, die Leistung auf der Ebene von Teilprozessen zu verstehen bzw. zu steuern und die Ergebnisse für das Management einzusetzen.

[4] Ein organisationsspezifischer Satz von Standardprozessen entspricht einer Sammlung von Definitionen von Prozessen, die die Aktivitäten in einer Organisation leiten. Diese Prozessbeschreibungen beinhalten die unabdingbaren Prozesselemente, die in definierte Prozesse aufgenommen werden müssen, die in Projekte, Arbeitsgruppen und bei Arbeiten über die Organisation hinweg eingesetzt werden [CMMI Project Team 2011, S. 457].

[5] Unter Tailoring versteht CMMI die Erstellung, Änderung oder Anpassung von etwas für einen bestimmten Zweck. Zum Beispiel etablieren Projekte oder Arbeitsgruppen ihre definierten Prozesse durch Tailoring des organisationsspezifischen Satzes von Standardprozessen für ihre Zielsetzungen, ihre Rahmenbedingungen und ihr Umfeld [CMMI Project Team 2011, S. 466].

Reifegrad 5 – Prozessoptimierung: Auf Reifegrad 5 verbessert eine Organisation kontinuierlich ihre Prozesse auf der Grundlage eines quantitativen Verständnisses ihrer Geschäftsziele und Leistungsbedürfnisse. Ein quantitativer Ansatz hilft, die inhärente Streuung im Prozess und die Ursachen von Prozessergebnissen zu verstehen. Schwerpunkt von Reifegrad 5 ist die kontinuierliche Verbesserung der Prozessleistung durch inkrementelle und innovative Technologie- und Prozessverbesserung. Die Qualitäts- und Prozessleistungsziele der Organisation sind etabliert und werden kontinuierlich überarbeitet, um Änderungen der Geschäftsziele und der Organisationsleistung widerzuspiegeln. Die ständig angepassten Ziele werden als Kriterien für das Management der Prozessverbesserung verwendet. Im Reifegrad 5 beschäftigt sich die Organisation mit der Gesamtleistung der Organisation und zieht dazu Daten aus mehreren Projekten heran. Aufgedeckte Mängel regen zu organisationsweiten Prozessverbesserungen an, welche wiederum für eine messbare Leistungsverbesserung sorgen.

2.2.3 Methoden zur Ermittlung von Reifegraden in der Praxis

Mit Hilfe eines sogenannten Appraisals kann ermittelt werden, auf welchem Reife- bzw. Fähigkeitsgrad sich ein Unternehmen befindet und wie entsprechende Prozesse verbessert werden können. Bei der Leistungsbewertung werden die Klassen A, B und C unterschieden, wobei die qualitative Aussagekraft und die methodische Formalisierung der Bewertung von A nach C abnimmt [Vgl. Gausemeier & Plass 2014, S. 321]. Appraisalmethoden der Klasse A erfüllen gleichzeitig die Anforderungen von ISO 15504 (SPICE) und werden als einzige vom Software Engineering Institute als ausreichend angesehen, um eine Aussage über die Reife einer Organisation zu machen. Die vom Software Engineering Institute definierte Methode für CMMI-Begutachtungen ist SCAMPI (Standard CMMI Appraisal Method for Process Improvement). SCAMPI-Begutachtungen dienen einerseits zur internen Prozessverbesserung und der Identifizierung von Verbesserungsmöglichkeiten. Andererseits können sie einem Auftraggeber dabei helfen, die Prozessreife eines potenziellen Auftragnehmers zu bewerten, was wiederum als Grundlage für die Vergabe eines Auftrages dienen kann.

Bei CMMI stellen höhere Reife- bzw. Fähigkeitsgrade grundsätzlich eine Verbesserung dar und sind somit im Allgemeinen erstrebenswert. Die Entscheidung welcher Fähigkeits- bzw. Reifegrad von einem Unternehmen angestrebt werden sollte, bleibt i.d.R. diesem jedoch selbst überlassen.

Kapitel 3

Theoretische Grundlagen zum Risikomanagement

3.1 Abgrenzung des Risikobegriffs

ISO 31000 definiert Risiko als die „Auswirkung von Unsicherheit auf Ziele“, wobei unter Auswirkung eine Abweichung von Erwartungen, sowohl in positiver als auch in negativer Hinsicht verstanden wird [ISO 31000 2009, S. 8]. Laut dieser Norm stellt Risiko somit die Möglichkeit dar, dass das tatsächliche Ergebnis einer unternehmerischen Aktivität von dem erwarteten Ergebnis positiv oder negativ abweicht.

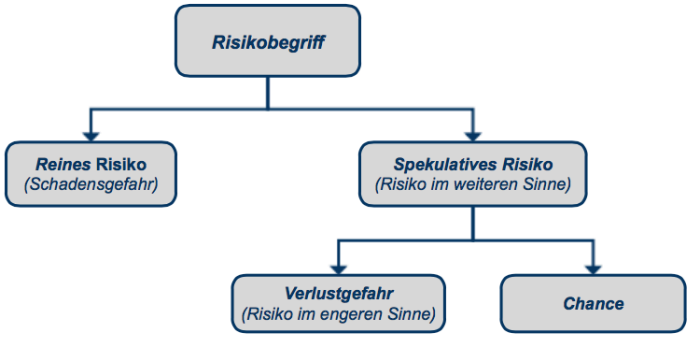


Abbildung 5: Reines und spekulatives Risiko [Vgl. Lück & Unmuth 2006, S.16]

Im Gegensatz zu der generischen Definition des Risikobegriffs in der ISO 31000 wird in der betriebswissenschaftlichen Literatur zwischen reinem und spekulativem Risiko unterschieden (Abbildung 5). Das reine Risiko beinhaltet Schadensgefahren, bei denen ein Ereignis eintritt, welches das Vermögen eines Unternehmens unmittelbar mindert. Dies beinhaltet ausschließlich die Gefahr des Vermögensverlustes, positive Abweichungen vom Erwartungswert werden dabei nicht erfasst. Im Gegensatz dazu umfasst das spekulative Risiko diejenigen unsicheren Ereignisse wel-

che sich durch unternehmerisches Handeln vermögensmindernd oder vermögensmehrend auswirken. Dabei wird die Möglichkeit einer Streuung des Zukunftserfolges, also sowohl eine positive als auch negative Abweichung vom Erwartungswert, als Risiko im weiteren Sinn bezeichnet [Vgl. Lück & Unmuth 2006, S.16].

Im Zuge dieser Arbeit wird in Anlehnung das COSO-ERM-Rahmenwerk zwischen Risiken und Chancen unterschieden. Demnach sind folgende Definitionen für die weitere Ausführung ausschlaggebend:

> *„**Risiko** ist die Möglichkeit, dass ein Ergebnis mit negativen Auswirkungen auf die Zielerreichung auftritt."*
>
> *„**Chance** ist die Möglichkeit, dass ein Ergebnis mit positiven Auswirkungen auf die Zielerreichung auftritt."*

Laut COSO II sind Risiken dabei Ereignisse mit negativen Auswirkungen, die Wertschöpfung verhindern oder bestehende Werte reduzieren können. Ereignisse mit positiven Auswirkungen können hingegen negative Effekte ausgleichen oder Chancen eröffnen. Chancen sind demnach Ereignisse, die das Erreichen von Zielen fördern und zur Wertschöpfung bzw. -erhaltung beitragen. Führungskräfte nutzen Chancen im Zuge ihres Strategie- und Zielsetzungsprozesses, indem sie die Nutzung der Chancen systematisch planen [COSO 2004, S. 16].

3.2 Unternehmensweites Risikomanagement nach COSO II

Im Jahr 2004 veröffentlichte COSO[6] das Enterprise Risk Management – Integrated Framework oder kurz COSO II bzw. COSO-ERM. Dieses Rahmenwerk geht von einer unternehmensweiten Betrachtung des Risikomanagements aus und definiert es wie folgt [COSO 2004, S. 16]:

> *„Unternehmensweites Risikomanagement ist ein Prozess, ausgeführt durch Überwachungs- und Leitungsorgane, Führungskräfte und Mitarbeiter einer Organisation, angewandt bei der Strategiefestlegung sowie innerhalb der Gesamtorganisation, gestaltet um die die Organisation beeinflussenden, möglichen Ereignisse zu erkennen, und um hinreichende Sicherheit bezüglich des Erreichens der Ziele der Organisation zu gewährleisten."*

[6] Die Abkürzung COSO steht für Committee of Sponsoring Organizations of the Treadway Commission.

3.2.1 Dimensionen des COSO II-Rahmenwerks

Das COSO II-Rahmenwerk baut auf dem ursprünglichen COSO I-Rahmenwerk (siehe Kapitel 4) auf, erweitert dieses jedoch nochmals um einige Elemente. Grundsätzlich folgt dieses Model einer dreidimensionalen Darstellung eines unternehmensweiten Risikomanagements, dargestellt in Abbildung 6. Dabei bezieht sich der COSO II-Würfel sowohl auf Zielkategorien (1. Dimension) und Komponenten (2. Dimension) des Risikomanagement-Systems als auch auf organisatorische Aspekte (3. Dimension) [Vgl. Denk et al. 2008, S. 54].

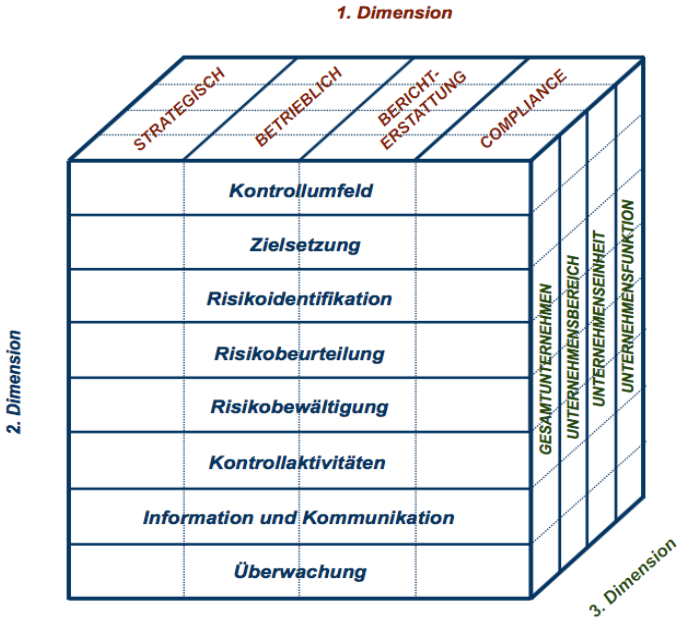


Abbildung 6: COSO II-Würfel [Denk et. al 2008, S. 53]

Im Rahmen der für eine Organisation festgelegten Mission oder Vision setzen Führungskräfte strategische Ziele fest und brechen diese auf die Ebenen der Organisation herunter. Daraus resultieren im Allgemeinen folgende vier Zielkategorien [COSO II, S. 23]:

- **Strategisch Ziele** sind Ziele auf hoher Ebene, die mit der Unternehmensmission abgestimmt sind und diese stützen. Das unternehmensweite Risikomanagement muss dabei einen starken Zukunftsbezug aufweisen.
- **Betriebliche Ziele** betreffen die Effektivität und Effizienz von Geschäftstätigkeiten, einschließlich Leistungs- und Gewinnziele bzw. Absicherung gegen den Verlust von Ressourcen. Hier weist das Risikomanagement häufig eine kurz- bis mittelfristige Perspektive auf.

- **Berichterstattung-Ziele** beziehen sich auf die Zuverlässigkeit der internen und externen Berichterstattung und können sowohl finanzielle als auch andere betriebliche Informationen beinhalten.
- **Compliance-Ziele** beziehen sich auf die Einhaltung gesetzlicher Anforderungen und selbstgesteckten Regulationen. Das Risikomanagement muss dabei einerseits auf regulatorische Anforderungen ausgerichtet sein, andererseits aber auch die Einhaltung von selbstgesteckten Standards des Unternehmens sicherstellen.

Des Weiteren besteht das unternehmensweite Risikomanagement aus acht wechselseitig verknüpften Komponenten. Diese leiten sich aus dem normalen Geschäftsablauf ab, sind in dem Managementprozess integriert und betrachten folgende Kernthemen [Vgl. COSO 2004, S. 22]:

- **Kontrollumfeld:** Das interne Umfeld beschreibt die Risikokultur einer Unternehmung und bildet die Grundlage dafür, wie Risiken durch die Mitarbeiter der Organisation betrachtet und behandelt werden.
- **Zielsetzung:** Das Vorhandensein klar spezifizierter Ziele ist eine notwendige Voraussetzung für die Identifikation von Ereignissen, die deren Erreichen beeinflussen können. Dabei ist die Vereinbarkeit der Zielsetzung mit der definierten Risikobereitschaft und -toleranzgrenze von großer Bedeutung.
- **Risikoidentifikation:** Interne und externe Ereignisse, die das Erreichen der Ziele einer Organisation beeinflussen, müssen bestimmt und in Risiken und Chancen unterschieden werden. Chancen gehen in den Strategiebildungs- oder Zielsetzungsprozess der Führungskräfte ein.
- **Risikobewertung:** Die Bewertung von Risiken muss unter Bezugnahme auf die definierten Unternehmensziele erfolgen und vor diesem Hintergrund die Voraussetzung für die Risikosteuerung legen.
- **Risikobewältigung:** Das Management wählt Instrumente zur Risikosteuerung (Vermeiden, Annehmen, Verringern oder Teilen von Risiko), um ein Bündel von Maßnahmen zum Anpassen der Risiken an die Risikotoleranz und -bereitschaft der Organisation festzulegen.
- **Kontrollaktivitäten:** Vorschriften und Verfahren, die sicherstellen, dass Risikoreaktionen wirksam ausgeführt werden, werden festgelegt und umgesetzt.
- **Information und Kommunikation:** Wesentlicher Bestandteil des Risikomanagements ist die Etablierung von Informationsflüssen, um sicherzustellen, dass die jeweiligen Mitarbeiter entsprechend ihrer Verantwortlichkeiten im Hinblick auf Identifikation, Bewertung und Steuerung von Risiken mit Informationen versorgt sind.

- **Überwachung:** Das gesamte Risikomanagement wird laufend überwacht und gegebenenfalls Anpassungen vorgenommen. Dadurch soll sichergestellt werden, dass das Risikomanagement dynamisch auf veränderte Umweltbedingungen reagieren kann.

3.2.2 Risikokategorisierung unter Heranziehen der Zielkategorien aus COSO II

Zusammenfassend handelt es sich bei COSO II um einen umfangreichen Standard, welcher Unternehmen beim Erreichen sowohl ihrer strategischen und betrieblichen Risiken als auch ihrer Berichterstattungs- und Compliance-Ziele unterstützt. Trotz einer teilweisen Überschneidung der Zielkategorien erlaubt diese Gliederung eine Fokussierung der einzelnen Teilaspekte des Risikomanagements [Vgl. Sommer 2010, S. 12].

Aufgrund der Tatsache, dass Risiken über Ereignisse mit negativen Auswirkungen auf die Zielsetzungen eines Unternehmens definiert werden, sollen die einzelnen Zielkategorien dafür herangezogen werden, um eine für die vorliegende Arbeit zweckmäßige Risikoeinteilung zu treffen (Abbildung 7).

Ausgehend vom sogenannten Unternehmenszweck, also der Vision und daraus abgeleiteten Mission eines Unternehmens, legt das Management strategische Ziele fest, formuliert Strategien und entwickelt daraus abgeleitete betriebliche Berichterstattungs- und Compliance-Ziele [COSO 2004, S. 35]. Zieht man an dieser Stelle die Risiko-Definition nach COSO II (Kapitel 3.1) heran, ergibt sich folgende Einteilung der Risikoarten, wobei jedes der vier Risikoarten für mögliche Ereignisse steht, welche die jeweiligen Zielsetzungen negativ beeinflusst:

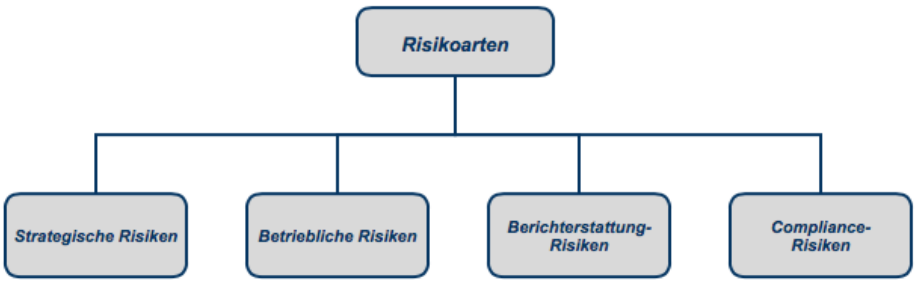


Abbildung 7: Risikokategorisierung

Strategische Risiken sind demnach Ereignisse, die dazu führen können, dass strategische Ziele verfehlt werden. In der Praxis resultieren diese Risiken aus Verkettungen verschiedener Unternehmensentscheidungen, wodurch sie die Realisierung der unternehmensweiten Strategie beeinträchtigen und somit möglicherweise den Erfolg oder gar den Bestand des Unternehmens gefährden [Vgl. Gleissner 2011, S. 65]. Strategische Risiken werden Fehlentscheidungen der höheren Managementebene zugeordnet und sind dadurch charakterisiert, dass sie relativ komplex sind und über einen längeren Zeitraum bestehen [Vgl. Haas 2007, S. 11].

Betriebliche Risiken sind Ereignisse, welche das Erreichen der operativen Ziele gefährden. Diese Risiken sind in der Regel unmittelbar mit den Geschäftsprozessen eines Unternehmens verknüpft. Aus diesem Grund ist eine Betrachtung der Geschäftsprozesse eines Unternehmens beim Umgang mit dieser Art von Risiken in der Regel unerlässlich.

Unter **Berichterstattungsrisiken** werden jene Ereignisse verstanden, welche eine verlässliche Berichterstattung innerhalb des Unternehmens in irgendeiner Art gefährden.

Compliance-Risiken stellen im Allgemeinen Verstöße gegen gesetzliche oder unternehmensspezifische Anforderungen dar.

3.3 Implementierung eines integrierten Risikomanagements nach ISO 31000

Im Jahr 2005 beschloss die International Standardization Organization (ISO) die Erarbeitung eines Standards zum Risikomanagement und verabschiedete im November 2009 die ISO 31000 „Risk Management – Principles and Guidelines“. Die Norm stellt Grundsätze und generische Richtlinien für die Implementierung eines Risikomanagement-Systems für private und öffentliche Organisationen zur Verfügung [Sommer 2010, S. 83]. Der Begriff des Risikomanagements ist weit gefasst und wie folgt definiert [ISO 2009, S. 9]:

> *„Koordinierte Aktivitäten zur Lenkung und Steuerung eine Organisation in Bezug auf Risiken“*

Abbildung 8 zeigt den grundlegenden Aufbau der Norm, welcher im Allgemeinen aus drei Teilen besteht. Im Zuge des ersten Teils werden die Grundsätze eines wirksamen Risikomanagements aufgezeigt, der im zweiten Teil beschriebene Rahmen bildet die Grundlage für die Umsetzung des Risikomanagements im Unternehmen und der dritte Teil beschreibt den eigentlichen Risikomanagement-Prozess. Die Implementierung nach ISO 31000 umfasst demnach sowohl den RM-Rahmen selbst als auch im rechten Teil dargestellten Risikomanagement-Prozess.

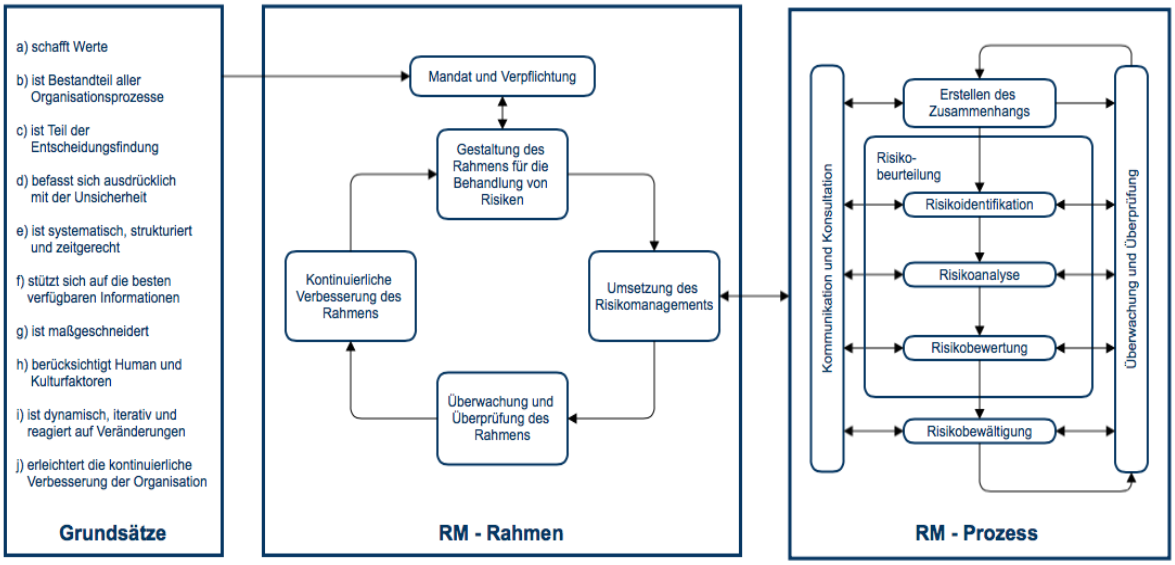


Abbildung 8: Komponenten der ISO 31000 (ISO 2009, S. 7)

3.3.1 Merkmale des Standards ISO 31000

Wesentlich an ISO 31000 ist, dass es sich bei ihr um eine allgemein gehaltene Basis-Norm handelt, welche Risikomanagement als Führungsaufgabe darstellt und einem umfassenden Top-Down-Ansatz folgt [Brühwiler & Romeike 2010, S. 83].

Umfassender Top-Down-Ansatz: Im Vordergrund steht ein umfassender Führungsansatz, der sich mit den positiven und negativen Auswirkungen von Unsicherheit auf Ziele einer Organisation oder eines Unternehmens befasst. So fokussiert Risikomanagement nach ISO 31000 nicht nur die strategischen, es schließt auch alle nachgelagerten Risiken auf operationeller und prozessualer Führungsebene ein. Abbildung 9 zeigt einen Top-Down-Ansatz, bei dem das operative Management die Ziele des strategischen Managements konkretisiert und die Leistungsprozesse aufzeigt, mit welchen Abläufen und Tätigkeiten die operationellen Ziele erreicht werden sollen. Somit besteht die einfache, aber entscheidende Aussage der ISO 3100 darin, dass Risikomanagement als Verpflichtung der obersten Leitung einer Organisation verstanden wird.

Abbildung 9: Top-Down- und Bottom-Up-Ansatz [Vergleich Brühwiler & Romeike 2010, S. 84]

Risikomanagement im Regelkreis der Führung: Eine Besonderheit von ISO 31000 besteht darin, dass es sich dabei um eine Führungsaufgabe handelt. Im Unterschied zu früheren Ansätzen, bei denen das Risikomanagement den Prozess der Risikobeurteilung in den Mittelpunkt stellte, betrachtet ISO 31000 den organisatorischen Rahmen für das Risikomanagement als gleichwertig. Die Führungsaufgabe ist demnach ein Regelkreis. Ein einfaches und weit verbreitetes Modell ist dafür der sogenannte Deming-Kreis, der die einander folgenden Tätigkeiten der Planung, Umsetzung, Bewertung und Verbesserung umfasst. Risikomanagement als Aufgabe der Führung soll also nicht als spontan und intuitiv verstanden werden, vielmehr soll es als Regelkreis mit einer vorgegebenen Abfolge von Führungsaktivitäten einem systematischen Ansatz folgen.

Eine allgemeine Basisnorm: Das dritte bedeutende Merkmal der ISO 31000 ist ihr generischer Aufbau. Sie ist sehr allgemein gehalten und stellt somit einen branchenübergreifenden Ansatz dar, welcher funktionsübergreifend angewendet werden kann.

3.3.2 Generischer Risikomanagement-Rahmen in der ISO 31000

Risikomanagement liegt in erster Linie in der Verantwortung der obersten Leitung, die die Risikostrategie und die Risikopolitik zu bestimmen hat. Dazu gehören explizit auch die Management-Aufgaben der Planung, Umsetzung, Bewertung und Verbesserung, was mit dem Deming-Kreis als P-D-C-A-Zyklus bezeichnet wird, dargestellt in Abbildung 10. ISO 31000 definiert damit detailliert die Gestaltung eines langfristig erfolgreichen und wirkungsvollen Risikomanagement-Systems.

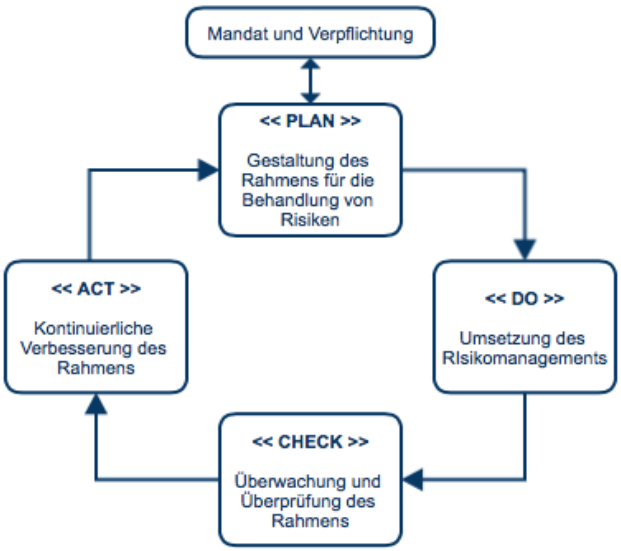


Abbildung 10: Generischer RM-Rahmen in ISO 31000 [Vgl. ISO 2009, S.17]

Die Aktivitäten im P-D-C-A-Kreislauf folgen den Vorgaben des Managements (Mandat und Verpflichtung), welches genau definiert, was mit Risikomanagement erreicht werden soll, wie dies erreicht werden soll, wie die Umsetzung geprüft werden soll und wie das System kontinuierlich verbessert werden soll. Basierend darauf wird im Anschluss der Rahmen des Risikomanagements festgelegt [Vgl. Wiendahl 2014, S.38]:

- **PLAN:** In der ersten Phase wird die Risikopolitik definiert und an den internen und externen Stakeholdern ausgerichtet. Im Zuge der Gestaltung der organisatorischen Rahmenbedingungen werden die Verantwortlichkeiten geklärt und der gewollte Integrationsgrad in bestehende Unternehmensabläufe geplant.
- **DO:** Die Umsetzung der gestellten Anforderungen durch das Management erfolgt mittels des RM-Prozesses und stellt demnach die zweite Phase im P-D-C-A-Kreislauf dar.
- **CHECK:** Im Sinne des Regelkreises erfolgt nun in der dritten Phase sowohl die Auswertung und Analyse der Ergebnisse als auch die Überprüfung der Angemessenheit an die aktuelle bzw. zukünftige Ausrichtung des Unternehmens.
- **ACT:** Im Zuge der dritten Phase werden durch eine kontinuierliche Verbesserung die Ergebnisse bewertet und basierend darauf eine etwaige Entscheidung zur Optimierung des Risikomanagement-Systems getroffen.

3.3.3 Generischer Risikomanagement-Prozess in der ISO 31000

Abbildung 11 zeigt den generischen RM-Prozess, der im Rahmen eines unternehmerischen Risikomanagements auf allen Ebenen und Funktionen durchgeführt werden sollte. Nachfolgend werden die einzelnen Schritte erläutert und im Speziellen auf die Risikoidentifikation, Risikoanalyse, Risikobewertung und Risikobewältigung eingegangen.

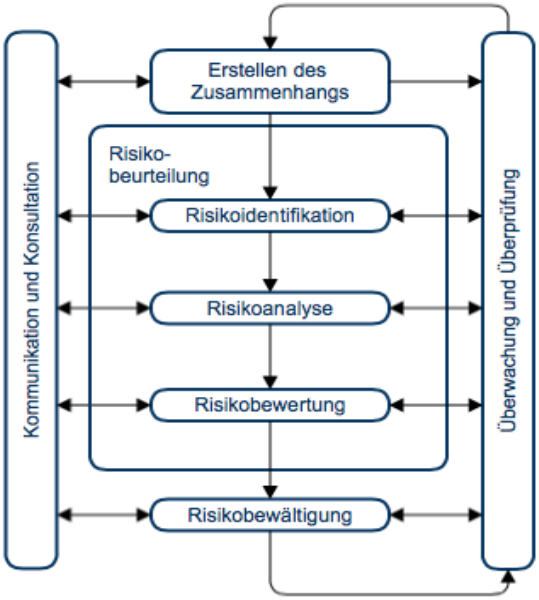


Abbildung 11: Generischer RM-Prozess in ISO 31000 [Vgl. ISO 2009, S.22]

Erstellung des Zusammenhangs: Im Zuge der Kontextdefinition werden für das Management von Risiken relevante interne und externe Einflussfaktoren bestimmt und der Geltungsbereich und die Risikokriterien[7] für den nachfolgenden RM-Prozess festgelegt [Vgl. ISO 2009, S. 23]. Angesichts der Kosten-Nutzen-Überlegung ist es weder möglich noch notwendig, sämtliche Risiken im Unternehmen zu analysieren. Es gilt daher sowohl den Umfang der Risikomanagementaktivitäten als auch die Risikobewertungskriterien bzw. Limit-Toleranzen festzulegen [Vgl. Sommer 2010, S. 85].

Wie in Abbildung 11 ersichtlich, fasst ISO 31000 den gesamten Prozess der Risikoidentifikation, Risikoanalyse und Risikobewertung unter dem Begriff Risikobeurteilung zusammen. Um Verwirrungen zu vermeiden, wird in der vorliegenden Arbeit jedoch die Verwendung dieses Begriffes vermieden und ausschließlich Bezug auf die folgenden drei Unterbegriffe genommen:

[7] Risikokriterien sind Bezugspunkte, zu welchem die Bedeutung eines Risikos bewertet wird. Sie beruhen auf Zielen des Unternehmens, sowie auf dessen internen und externen Umfeld und können aus Normen, Gesetzen, Politiken und anderen Anforderungen abgeleitet werden [ISO 31000 2009, S.13].

Risikoidentifikation

Die Risikoidentifikation beschäftigt sich mit der Erfassung aller für das Unternehmen wesentlicher Einzelrisiken, wobei nicht nur bereits bestehende, sondern auch zukünftig mögliche Risiken zu identifizieren sind [Vgl. Brühwiler & Romeike 2010, S. 149]. In diesem Zusammenhang betont die internationale Norm ISO 31000 die Bedeutung der Ziele einer Organisation, da diese als Ausgangspunkt für die Risikoidentifikation dienen. Des Weiteren sollte die Risikoidentifikation Instrumente und Methoden einsetzen, die ihren Zielen und Fähigkeiten sowie den auftretenden Risiken angemessen sind [Vgl. ISO 31000 2009, S.26].

Risikoanalyse

Schwerpunkt der Risikoanalyse ist die Entwicklung eines Verständnisses für jedes Risiko. Demnach muss gewährleistet sein, dass entsprechende Kenntnisse über plötzlich eintretende Ereignisse, ihre Ursachen und Auswirkungen auf die Ziele vorhanden sind, um einen adäquaten Umgang zu gewährleisten [Vgl. Brühwiler 2007, S. 98]. Somit bildet die Risikoanalyse die Grundlage für Entscheidungen, ob und wie Risiken behandelt werden und welche Behandlungsstrategien und -verfahren dafür geeignet sind. In diesem Zusammenhang ist sowohl die potenzielle positive oder negative Auswirkung eines Ereignisses oder Umstandes, als auch die entsprechende Eintrittswahrscheinlichkeit von Bedeutung. Mit Hilfe dieser beiden Dimensionen kann dann ein geeignetes Risikoniveau[8] quantifiziert werden [Vgl. ISO 31010 2009, S. 11]. Dazu findet in der Praxis eine große Anzahl an unterschiedlichen Verfahren Anwendung, welche sich im Allgemeinen in qualitative und quantitative Methoden unterteilen lassen.

Risikobewertung

In der Risikobewertung werden die qualitativen und quantitativen Parameter von Risiken mit den entsprechenden Risikokriterien der Organisation verglichen [ISO 31000 2009, S.27]. Das Ziel dieser Phase besteht darin, die ursächlichen Strukturen und möglichen Interdependenzen der Risiken transparent zu machen und ihre Wirkungen soweit wie möglich quantitativ offen zu legen [Denk et al. 2008, S.102]. Somit schafft die Bewertung eine Priorisierung der Risiken nach den Kriterien der Organisation, wodurch ein entsprechender Handlungsbedarf abgeleitet werden kann [Vgl. ISO 2009, S. 27].

[8] Unter Risikoniveau wird das Ausmaß eines oder mehrerer Risiken verstanden, das als bestimmte Kombination von Auswirkung(en) und Eintrittswahrscheinlichkeit(en) zum Ausdruck gebracht wird [ISO 31000, S. 13].

Risikobewältigung

In dieser Phase des RM-Prozesses werden geeignete Maßnahmen ausgewählt, um die zuvor bewerteten Risiken zu bewältigen [ISO 2009, S. 28]. Abbildung 10 gibt einen grafischen Überblick verschiedener Möglichkeiten zur Risikobewältigung. Dabei gestaltet und beeinflusst die aktive Risikobewältigung die Risikostruktur mit dem Ziel, Eintrittswahrscheinlichkeit und/oder Tragweite von Risiken zu reduzieren. Die passive Risikobewältigung lässt hingegen die Risikostruktur unverändert, beeinflusst also weder Eintrittswahrscheinlichkeit noch Schadensausmaß und hat vielmehr das Ziel, die finanziellen Auswirkungen für das Unternehmen zu reduzieren [Denk et al. 2008, S.128].

Im Rahmen der vorliegenden Arbeit wird jedoch von dieser Unterteilung abgesehen und vielmehr zwei Arten von Maßnahmen zur Risikobewältigung unterschieden: **Steuerungs-** und **Kontrollmaßnahmen**. Dabei beziehen sich Steuerungsmaßnahmen auf die Bewältigung von Risiken auf strategischer Ebene im Zuge eines Chancen- und Risikomanagements und adressieren im Allgemeinen strategische und finanzielle Risiken mit hoher Komplexität. Demgegenüber kommen in den operativen Bereichen eines Unternehmens vorwiegend Kontrollmaßnahmen zum Einsatz um Schwachstellen zu reduzieren bzw. zu eliminieren. Kontrollmaßnahmen adressieren demnach vorwiegend Risiken im engeren Sinne [Vgl. Hunziger 2012 S. 3].

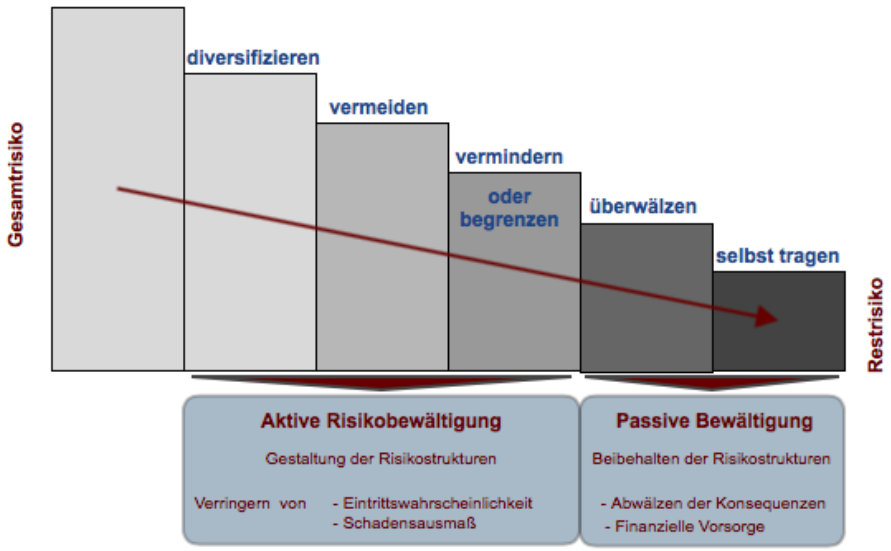


Abbildung 12: Möglichkeiten der Risikobewältigung [Vgl. Denk et al. 2008, S. 130]

Im Zuge der Risikobewältigung ist darauf zu achten, dass die ergriffenen Maßnahmen selbst Risiken herbeiführen können und dass die Ineffektivität des Risikomanagement-Systems ebenfalls ein wesentliches Risiko darstellt [Sommer 2010, S. 86].

Parallel zu den oben beschriebenen Prozessschritten erfolgen die Kommunikation und Konsultation bzw. die Überwachung und Überprüfung der Ergebnisse der einzelnen Schritte. **Kommunikation und Konsultation** sollen sicherstellen, dass die Verantwortlichen die Entscheidungsgrundlagen und die notwendigen Handlungen verstehen. Durch das Einbeziehen verschiedener interner und externer Stakeholder tragen deren unterschiedliche Perspektiven und Fachkenntnisse dazu bei, Risiken situationsgerecht zu identifizieren. **Überwachung und Überprüfung** der einzelnen Prozessschritte stellen hingegen die Wirksamkeit des RM-Systems sicher und dienen der Erkennung von Änderungen im internen und externen Umfeld sowie der Änderung von bereits identifizierten Risiken [Vgl. Sommer 2010, S. 86].

3.4 Three Lines of Defense: Referenzmodell zur Anordnung der RM-Funktionen

Die Rollenverteilung in Bezug auf Risikomanagement- und Kontrolltätigkeiten werden 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. In diesem Zusammenhang veröffentlichte der Dachverband der europäischen Revisionsinstitute (ECIIA) in einem Positionspaper das Three Lines of Defense Model for Internal Governance, um die Wechselwirkungen zwischen den verschiedenen Akteuren im Risikomanagement strukturiert zu beschreiben [Vgl ECIIA 2013, S. 1]. Das in Abbildung 13 dargestellte Three Lines of Defense Modell bietet eine einfache und kompakte Darstellung der Rollenverteilung der einzelnen RM-Funktionen im Unternehmen. Im Zuge der vorliegenden Arbeit soll es als Referenzmodell dienen, um die Anordnung der einzelnen Risikomanagement-Funktionen im Unternehmen zu beschreiben und die Bereiche klar abzugrenzen.

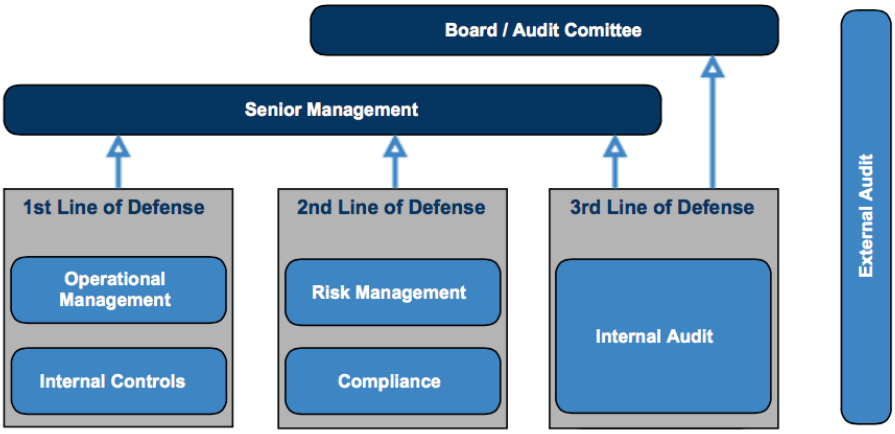


Abbildung 13: Three Lines of Defense Modell [Vgl. ECIIA 2013, S. 2]

- Die **1st Line of Defense** bildet das operative Management, welches für die Sicherstellung der Identifizierung, Beurteilung und Kontrolle der Risiken im Rahmen des Tagesgeschäfts verantwortlich ist.
- Im Zuge der **2nd Line of Defense** ermöglicht die RM-Funktion die Umsetzung wirksamer RM-Methoden und unterstützt die Risikoeigner[9] vor allem bei der Definition von Zielvorgaben innerhalb der Organisation. In einigen Unternehmen wird für die Überwachung von Compliance-Risiken zusätzlich auch eine separate Compliance-Funktion eingerichtet.
- Die **3rd Line of Defense** stellt als objektive und unabhängige Prüfungs- und Beratungsinstanz die Interne Revision dar, welche die Geschäftsleitung, Führungskräfte und Überwachungsinstanzen unterstützt und Sicherheit über die Angemessenheit und Wirksamkeit der Überwachungs-, Risikomanagement- und Kontrollstrukturen gibt [Vgl. ECIIA 2013, S. 2].

[9] ISO 31000 versteht unter einem Risikoeigner jene Person oder Stelle im Unternehmen mit der Verantwortung und Befugnis, hinsichtlich eines Risikos zu handeln [ISO 31000, S. 10].

Kapitel 4

Ausgestaltung des 3LoD-Modells im Unternehmen

4.1 Abgrenzung der einzelnen RM-Funktionen im 3LoD-Modell

Abbildung 14 zeigt alle organisatorischen Abteilungen, welche in der Regel in mittleren und größeren Unternehmen implementiert und für die Bewältigung unterschiedlicher Risiken verantwortlich sind. Im Zuge dieser Arbeit werden diese Bereiche als RM-Funktionen bezeichnet. RM-Funktionen sind demnach jene organisatorischen Abteilungen im Unternehmen, welche bewusst oder unbewusst mit ihrem Tun und Handeln einen positiven Beitrag zum unternehmensweiten Risikomanagement leisten.

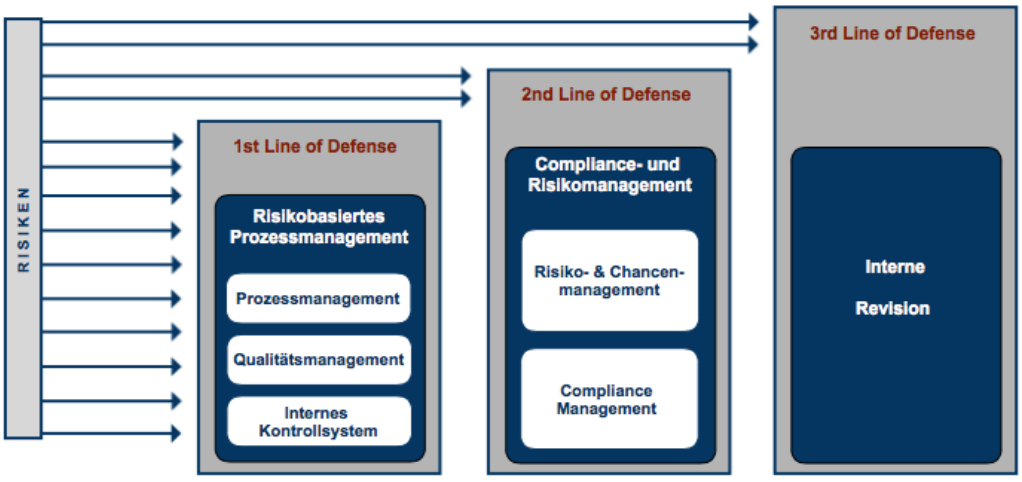


Abbildung 14: Abgrenzung der RM-Funktionen im Unternehmen

- Im Zuge der **1st Line of Defense** sind das Prozessmanagement (PM), das Qualitätsmanagement (QM) und das Interne Kontrollsystem (IKS) für die Sicherstellung der Identifikation, Beurteilung und Kontrolle der Risiken im Rahmen des Tagesgeschäfts verantwortlich. Dieser vorwiegend operative Bereich des Risikomanagements wird in der vorliegenden Arbeit als risikobasiertes Prozessmanagement (rPM) verstanden.
- Im Gegensatz zur 1st Line of Defense werden von der **2nd Line of Defense** jene Risiken adressiert, welche auf sehr hohem Niveau und unmittelbaren Bezug zu den Unternehmenszielen stehen. Sowohl das Risiko- & Chancenmanagement (RCM) als auch das Compliance-Management (CM) sind für jene Risiken im Unternehmen verantwortlich, die aufgrund ihrer hohen Komplexität nicht alleine durch Kontrollen zu bewältigen sind, sondern ausgewählter Maßnahmen der Risikosteuerung bedürfen. Im Sinne einer 2nd Line of Defense werden diese beiden RM-Funktionen in der vorliegenden Arbeit zum Risiko- & Compliancemanagement (RMCM) zusammengefasst.
- Die Interne Revision (IR) überwacht als sogenannte **3rd Line of Defense** die Einhaltung der etablierten Kontrollen des rPM sowie die Wirksamkeit der Steuerungsmaßnahmen des C-&RM oder deckt bereits eingetretene Schäden auf. Die IR agiert unabhängig von den RM-Funktionen und berichtet direkt an den Vorstand bzw. indirekt an den Aufsichtsrat.

Erst das Zusammenwirken dieser drei Lines of Defense unterstützt einen wirkungsvollen Umgang mit Risiken im Sinne eines unternehmensweiten Risikomanagements. In der weiteren Ausführung dieser Arbeit ist das risikoorientierte Prozessmanagement im Sinne einer First Line of Defense für den Umgang mit Risiken im Zuge des Tagesgeschäfts verantwortlich, das Risiko- & Compliancemanagement wird hingegen als strategische Komponente gesehen und die Interne Revision als Prüforgan der beiden vorigen verstanden.

4.2 First Line of Defense: Risikoorientiertes Prozessmanagement

Im Folgendem wird aufgezeigt, wie PM, QM und IKS im Unternehmen aufgebaut sein können, wie die RM-Funktionen voneinander abzugrenzen sind und welche Synergien sie aufweisen. Dabei wird speziell auf deren Ziele eingegangen, um die daraus resultierenden Risiken voneinander abgrenzen zu können.

4.2.1 Prozessmanagement

Die Suche nach einer geeigneten Definition von Prozessmanagement in der gängigen Literatur gestaltet sich schwierig, da in den meisten Fällen lediglich eine Definition des Prozesses und gelegentlich die Einführung der Prozessorientierung zugrundeliegenden Probleme im Vordergrund stehen. Im Zuge dieser Arbeit hat sich in Anlehnung der Literaturrecherche von Kruse [2009, S. 58] im Hinblick auf das weitere Prozedere die folgende Definition als zweckdienlich erwiesen:

> *„Prozessmanagement ist das zielorientierte Gestalten und Lenken von Geschäftsprozessen, welches mit planerischen, organisatorischen und kontrollierenden Maßnahmen sowie mit einer personen- und sachbezogenen Komponente wesentlich zur Optimierung der unternehmerischen Wertschöpfungskette beiträgt.“*

Es sei jedoch an dieser Stelle auf die Wichtigkeit einer prozessorientierten Unternehmensführung hingewiesen, da sie den Kern eines erfolgreichen Prozessmanagements darstellt. Dabei wird unter Prozessorientierung die Grundhaltung verstanden, bei der das gesamte betriebliche Handeln als Kombination von Prozessen beziehungsweise Prozessketten betrachtet wird [Kuhlang 2013].

Abbildung 15: Schematische Prozesslandkarte im Unternehmen [Vgl. Wagner & Käfer 2013, S. 40]

Ziele des Prozessmanagements und die daraus abgeleiteten Risiken

Beim Prozessmanagement steht somit die **effektive und effiziente Umsetzung aller unternehmerischen Prozesse** im Mittelpunkt. Das systematische an der Vision und den Strategien ausgerichtete Optimieren des Zusammenspiels dieser Prozesse im Sinne eines Führungssystems mit klarer Verantwortung stellt dabei sicher, dass die Organisation ihre Ziele erreicht. Ausgehend von der Prozesslandkarte (Abbildung 15) über die Gestaltung der Prozesse und deren Optimierung auf Basis der verursachten Prozesskosten unterstützt das Prozessmanagement die Entwicklung zur Realisierung einer prozessorientierten Organisation [Wagner & Käfer 2013, S. 36].

Hauptziel des klassischen Prozessmanagements liegt neben der Strategieverbindung vor allem in der **Effektivität und Effizienz der unternehmensweiten Prozesse**, gemessen anhand von Prozesszielen, der Schnittstellenoptimierung im Sinne eines zu erreichenden Gesamtoptimums sowie der Dokumentation und Überwachung dieser Prozesse zur Systemsteuerung [Wagner & Käfer 2013, S. 16].

Im Zuge der vorliegenden Arbeit werden demnach alle Risiken, welche die Effektivität bzw. Effizienz der unternehmerischen Prozesse in irgendeiner Art beeinträchtigen und im Unternehmen im Zuge des Prozessmanagements kontrolliert werden können, als **Prozessleistungsrisiken** bezeichnet. Ausschlaggebend ist dabei das Nichterreichen eines bestimmten Ablaufes bzw. das Nichterreichen eines vorgegebenen Prozess-Outputs.

4.2.2 Qualitätsmanagement

Im 20. Jahrhundert hat sich das Konzept des Qualitätsmanagements stetig weiterentwickelt. Lag zunächst vorwiegend der Schwerpunkt auf der Qualitätskontrolle und somit darauf, erzielte Qualität zu überprüfen, folgte mit der Weiterentwicklung des Qualitätsbegriffs auch die Einführung detaillierter Methoden, wie die Qualitätssicherung, das Qualitätsmanagement und schließlich das sogenannte umfassende Qualitätsmanagement, auch Total-Quality-Management (TQM) genannt [Vgl. Ertl-Wagner et al. 2009, S. 11]. Die internationale Norm ISO 9000 [2000, S. 21] versteht unter dem Begriff Qualitätsmanagement

> *„ ... aufeinander abgestimmte Tätigkeiten zum Leiten und Lenken einer Organisation bezüglich Qualität. Dies umfasst üblicherweise das Festlegen der Qualitätspolitik, Qualitätsziele, Qualitätsplanung, Qualitätslenkung, Qualitätssicherung sowie Qualitätsverbesserung."*

Diese Definition wird nun um den umfassenden Qualitätsbegriff nach ISO 9001 ergänzt, welcher laut der Norm die Basis eines prozessorientierten Ansatzes zur Organisation und Steuerung eines

Unternehmens darstellt. Dieser in Abbildung 16 dargestellte Qualitätsbegriff ist geprägt vom Wandel des ergebnisbezogenen Zugangs hin zum kunden- und prozessbezogenen. Die Qualität der Produkte und Dienstleistungen werden durch die Ansprüche der Kunden und des Marktes gesteuert. Dieser geforderte Qualitätsanspruch an Produkte und Dienstleistungen seitens der Kunden stellt wiederum Bedingungen an die Prozesse des Unternehmens. Um die Prozesse marktgerecht zu betreiben, muss passendes Potenzial vorhanden sein. Die Qualität des Produktes oder der Dienstleistung kann demnach nur dann in vollem Umfang zur Geltung kommen, wenn für den Kunden auch die Qualität des Prozesses an den Berührungspunkten mit dem Kunden in Ordnung ist. [Wagner & Käfer 2013, S. 119].

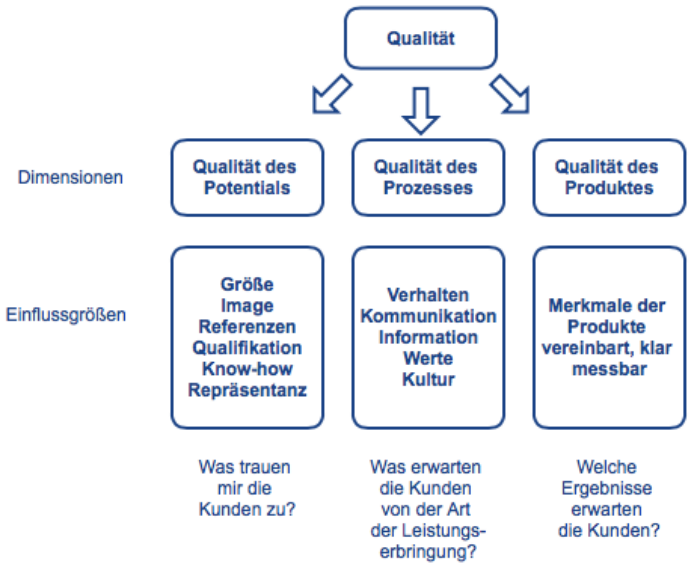


Abbildung 16: Dimensionen des umfassenden Qualitätsbegriffs [Vgl. Wagner & Käfer 2013, S. 120]

Die Orientierung hin zum umfassenden Qualitätsmanagement rückte das Qualitätsbewusstsein in den Mittelpunkt des Denkens. Ein wichtiger Kernbegriff des TQM ist die kontinuierliche Verbesserung und somit die unablässige Optimierung der Prozesse in einem Unternehmen. Im Rahmen des TQM werden die Beziehungen zwischen Kunden und Lieferanten innerhalb und außerhalb der Organisation genau definiert. Ziel ist ein vorausschauendes und integriertes Qualitätsmanagement.

Ziele des Qualitätsmanagements und die daraus abgeleiteten Risiken

Im Allgemeinen dient Qualitätsmanagement also der Optimierung des Kosten-Nutzen-Verhältnisses. Es zielt jedoch nicht zwangsläufig auf ein höherwertiges Endprodukt, sondern stellt die Erreichung eines vorgegebenen Qualitätsstandards sicher. Demnach kann auch ein Billigprodukt das Resultat eines vollständig qualitätskontrollierten Prozesses sein, dessen Qualitätsparameter eben entsprechend niedrig sind [Vgl Ertl-Wagner et al. 2009, S. 14].

Im Unterschied zum output- und ablauforientierten Prozessmanagement liegt die Hauptaufgabe des QM darin, dass alle qualitativen Anforderungen an Produkte, Prozesse und Potenziale berücksichtigt und erfüllt werden. Dabei können qualitative Anforderungen entweder explizit definiert vorliegen (z.B. als Arbeitsanweisung oder interne Richtlinie) oder implizit vorausgesetzt werden (z.B. unausgesprochene Kundenanforderung) [Schneider et al. S 21]. Demnach liegt der Fokus des QM neben der Konformität zu diversen Normen (z.B.: ISO 9100) auch bei der Sicherstellung der Kundenzufriedenheit und bei der Dokumentationslenkung zur Nachvollziehbarkeit [Vgl. Wagner & Käfer 2013, S.16]. Das QM führt nicht zwangsläufig zu mehr Effektivität und Effizienz der Prozesse, sondern steuert lediglich die Erreichung der vorgegebenen Qualitätsziele und ist vorwiegend kundenorientiert und methodisch.

Risiken, welche das Erreichen qualitativer Anforderungen an Produkte, Prozesse und Potenziale eines Unternehmens gefährden, werden im Zuge der vorliegenden Arbeit als **Produkt-, Prozess-** und **Potenzialqualitätsrisiken** bezeichnet und können im Allgemeinen im Zuge des Qualitätsmanagements behandelt werden.

4.2.3 Internes Kontrollsystem

Das Interne Kontrollsystem (IKS) basiert auf dem im Angloamerikanischen entstandenen Begriff **Internal Control**, dessen Entstehung in starkem Maße als Reaktion auf Betrugs- und Unterschlagungsfälle in der amerikanischen Wirtschaft zu sehen ist. Des Weiteren sollte die Internal Control menschliche Unzulänglichkeiten bei der Aufgabenerfüllung verhindern bzw. aufdecken [Klinger & Klinger 2009, S. 4]. Laut Sommer [2007, S. 20] lässt sich Internal Control zusammenfassend wie folgt umschreiben:

> *„Internal Control umfasst in die Geschäftsaktivitäten integrierte Prozesse sowie weitere Maßnahmen und Strukturen, die darauf ausgerichtet sind, Ergebnisse, welche die Unternehmenszielerreichung beeinträchtigen könnten, zu steuern, kontrollieren und Korrekturmaßnahmen einzuleiten und so die Wahrscheinlichkeit der Zielerreichung zu erhöhen."*

Der Begriff des Internal Control Systems wurde im deutschsprachigen Raum mit **Internen Kontrollsystem (IKS)** übersetzt. Dabei geht es um die Gestaltung eines Internen Steuerungs- und Überwachungssystems für alle wesentlichen Geschäftsprozesse eines Unternehmens. Welche Geschäftsprozesse wesentlich sind, hängt von dem jeweiligen Geschäftsmodell des Unternehmens ab [Vgl. Bungartz 2011, S. 45]. Dabei ist durch geeignete IKS-Kontrollen dafür zu sorgen, dass dolose Handlungen von Mitarbeitern vermieden oder zumindest erschwert werden und Gefahren aus mangelndem Kontrollbewusstsein, Vertrauensseligkeit oder Betriebsblindheit erkannt und nicht unterschätzt werden. [Vgl. Klinger & Klinger 2009, S. 8].

COSO I-Rahmenwerk als Referenz zur Ausgestaltung eines IKS

Trotz intensiver Auseinandersetzung mit dem Thema IKS in Forschung und Praxis besteht keine Einigkeit darüber, wie ein IKS aufgebaut und welche Ziele mit einem IKS verfolgt werden sollen. Ein relativ breit akzeptiertes IKS-Verständnis rührt aus dem 1992 in den USA publizierten COSO-Rahmenwerk für Interne Kontrolle, kurz COSO I, welches Unternehmen als Unterstützung bei der Bewertung und Verbesserung der internen Kontrollen dienen soll [Hunziger et al. 2012, S. 17].

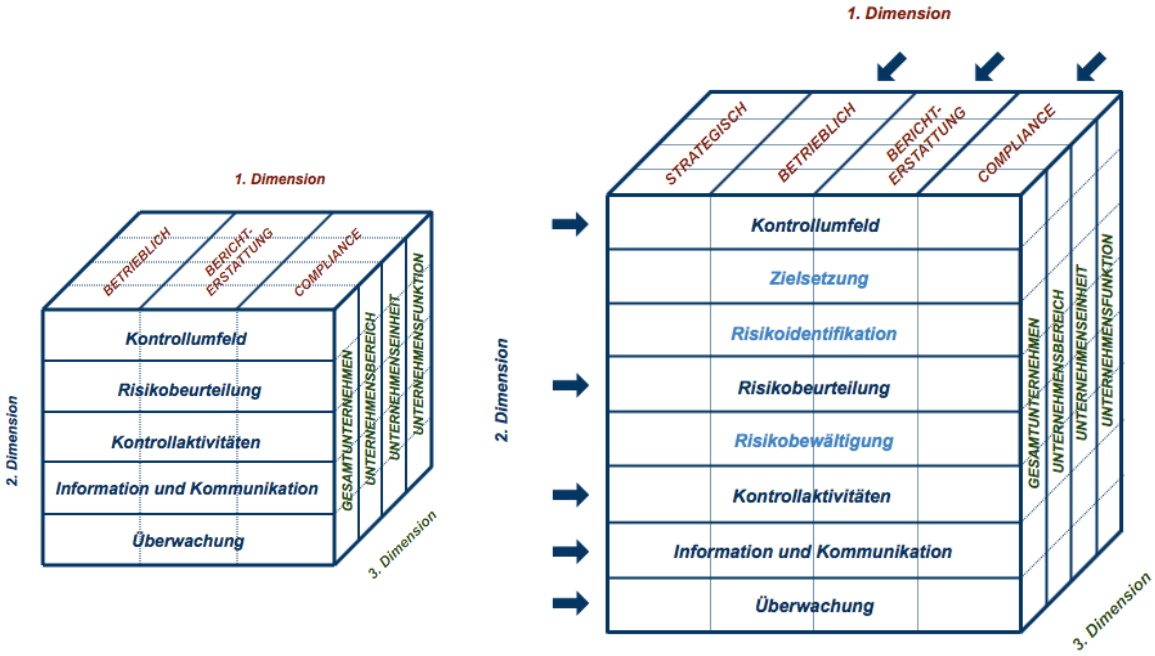


Abbildung 17: Vergleich COSO I und COSO II [www.coso.org]

Aus Abbildung 17 ist ersichtlich, dass bei COSO II das IKS als wesentlicher Bestandteil eines unternehmensweiten Risikomanagements verstanden wird [Vgl. Bungartz 2011, S. 47]. Im Vergleich zu COSO I finden bei COSO II eine verstärkte Fokussierung auf Risiken statt, indem einerseits zusätzlich die Strategieebene aufgenommen wird und andererseits die Risikobeurteilung explizit um die Elemente „Zielsetzung“, „Risikoidentifikation“ und „Risikobewältigung“ ergänzt wird. COSO II adressiert somit sowohl Risiken als auch Chancen und basiert demzufolge auf einem Risikobegriff im weiteren Sinne. Das IKS beschränkt sich hingegen im Allgemeinen auf eine reine Risikobetrachtung – Chancen werden in der Praxis kaum adressiert. Dem IKS liegt somit der Risikobegriff im engeren Sinne zugrunde und folglich der Schwerpunkt auf der Sicherstellung der Einhaltung von Maßnahmen im Zuge einer Schadensbegrenzung [Vgl. Schmid & Stäbler 2007, S. 642].

Die wesentlichen Risikobereiche des IKS liegen im Unternehmen dort, wo verwertbare oder verwendbare Güter vorhanden sind. Beispiele solcher Güter sind Geld, geldähnliche Werte, Handelswaren, aber auch Werkzeuge oder Kleinmaschinen. Gefährdet sind auch Forderungen an Kunden, Geschäftsgeheimisse, Kundenadressen, Know-How und Software. Vorwiegend kommen dolose Handlungen in folgenden Unternehmensbereichen vor [Klinger & Klinger 2009, S. 19]:

- Einkauf und Verkauf
- Wareneingang, Produktion, Lager- und Materialwirtschaft
- Buchhaltung und EDV
- überall wo fakturiert und verrechnet wird
    - Interne Lieferungen und Leistungen
    - Gutschriften, Spesenabrechnungen etc.

Internes Kontrollsystem mit engem und breitem Fokus

Bei der Bestimmung des Zielumfangs bedienen sich regulatorische Bestimmungen oftmals einer eingeschränkten Definition der Zielvorgaben, bei welcher das interne Kontrollsystem nur die Verlässlichkeit der finanziellen Berichterstattung zu gewährleisten hat. Diese Sichtweise wird in der vorliegenden Arbeit als IKS mit engem Fokus bezeichnet. Demgegenüber steht eine ganzheitliche Auslegung der Ziele und das daraus resultierende IKS mit breitem Fokus bzw. IKS nach COSO I (Abbildung 18). Das IKS mit breitem Fokus beinhaltet im Sinne von COSO I sowohl die allgemeine Berichterstattung (BERICHTERSTATTUNG) als auch die wirksame und effiziente Ausgestaltung von operativen Geschäftsprozessen (BETRIEBLICH) sowie die Gesetzes- und Normenkonformität (COMPLIANCE).

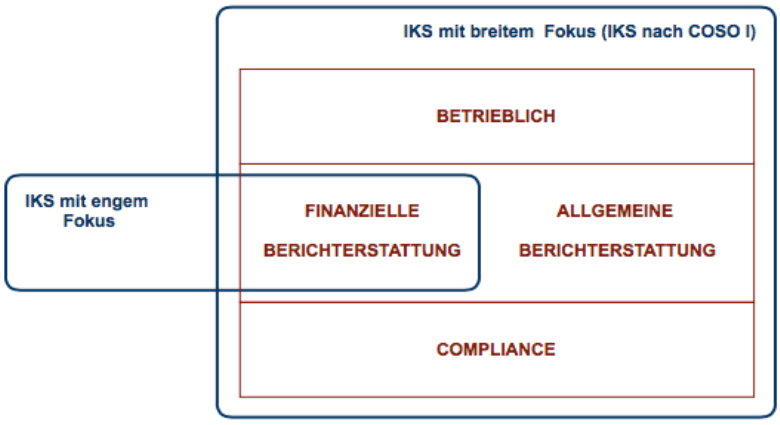


Abbildung 18: Internes Kontrollsystem mit engem und breiten Fokus [Vgl. Sommer 2007, S. 20]

Ziele des IKS und die daraus abgeleiteten Risiken

Das **IKS mit engem Fokus** zielt in der Regel weder auf die Effizienz noch auf die Qualität von Prozessen oder Dienstleistungen ab, sondern auf die Wirksamkeit der vorwiegend finanziellen Berichterstattung [Hunziger 2012, S. 33]. Demnach liegt die Hauptaufgabe des IKS mit engem Fokus darin, jene mit der Geschäftstätigkeit verbundenen Risiken abzuwenden, welche sich direkt aus Unregelmäßigkeiten in der Buchhaltung oder Bilanz des Unternehmens ableiten.

Demgegenüber adressiert ein **IKS mit breitem Fokus** die sowohl aus der finanziellen als auch allgemeinen Berichterstattung resultierenden Risiken und jene, welche sich im Zuge des Tagesgeschäfts aus der Gefährdung der betrieblichen Ziele und Compliance-Ziele ableiten lassen. An dieser Stelle können somit klare Synergien zum Prozess- und Qualitätsmanagement hergestellt werden, da ein IKS mit breitem Fokus sich den gleichen Risiken gegenübersieht wie das Prozess- und Qualitätsmanagement [Vgl. Sommer 2007, S. 20].

4.2.4 Risiken im risikobasierten Prozessmanagement

Aus den vorigen Kapiteln können nun, wie in Abbildung 19 dargestellt, den einzelnen RM-Funktionen die jeweiligen Risiken zugeordnet werden. Daraus ist ersichtlich, dass einige dieser Risiken von mehreren RM-Funktionen adressiert werden können.

An dieser Stelle sei auf die unterschiedliche Ausbauart der einzelnen RM-Funktionen im Unternehmen hingewiesen. Unternehmen mit einem stark ausgebauten bzw. zertifizierten Qualitätsmanagement-System sehen meist von einem Prozessmanagement ab. Da gängige Qualitätsmanagement-Normen, wie zum Beispiel die ISO 9001, einen prozessorientierten Ansatz fordern, wäre ein Prozessmanagement demnach obsolet. Demgegenüber können Unternehmen mit einem entsprechend leistungsstarken Prozessmanagement auch sämtliche Qualitätsrisiken bewältigen. Wie Abbildung 19 zeigt, kann ein gut aufgestelltes IKS mit breitem Fokus zur Gänze allen Risiken aus dem Prozess- und Qualitätsmanagement begegnen.

Somit ist es nicht wichtig, mit welcher RM-Funktion den einzelnen Risiken begegnet wird, sondern dass ein Unternehmen ihnen begegnet.

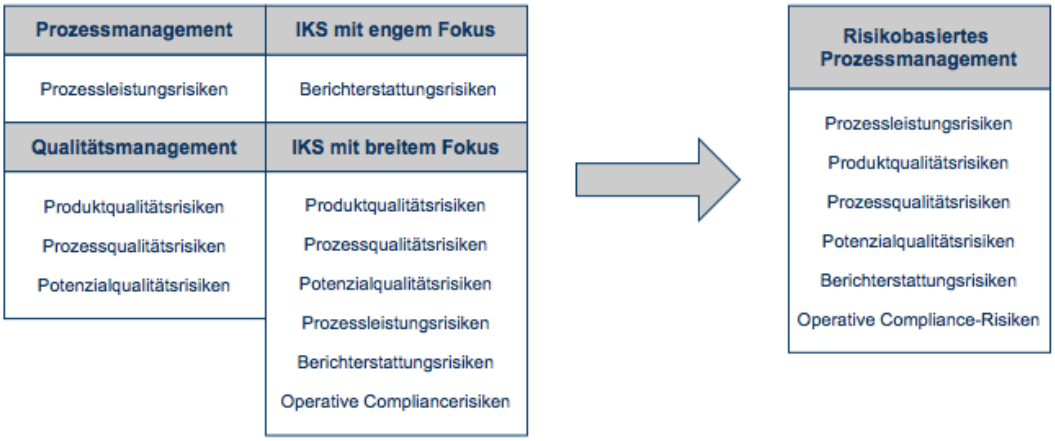


Abbildung 19: Risiken im risikobasierten Prozessmanagement

4.3 Second Line of Defense: Risiko- & Compliancemanagement

4.3.1 Risiko- & Chancenmanagement

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 die Erreichung und Sicherung einer risikooptimalen Unternehmensposition angestrebt werden [Vgl. Hoffmann 2012, S. 59]. Statt der Minimierung von Risiken liegt die Aufgabe eines erfolgreichen Risiko- & Chancenmanagements vor allem in der Schaffung von Transparenz über die Risikosituation im Unternehmen und dem optimalen Umgang mit den identifizierten Risiken [Vgl. Gleissner 2011, S.12]. Im Kontext des Risiko- & Chancenmanagements ist somit das spekulative Risiko von großer Bedeutung und insbesondere folgende vier Fragen ausschlaggebend [Vgl. Brühwiler 2007, S. 30]:

- **Welche Faktoren bedrohen Erfolg und Erfolgspotenziale?**
  Erfolgspotenziale, wie Kernkompetenzen, interne Stärken und Wettbewerbsvorteile, sind Voraussetzung 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.

- **Welche Eigenkapitalausstattung ist als „Risikodeckungspotenzial" nötig?**
  Die erforderliche Eigenkapitalausstattung eines Unternehmens ist vom Risikoumfang abhängig. Das Eigenkapital ist letztlich das Risikodeckungspotenzial eines Unternehmens, das die aggregierten Auswirkungen aller Risiken zu tragen hat.
- **Welches Performancemaß ist Basis der Unternehmenssteuerung?**
  Ein positiver Beitrag zum Unternehmenswert erfordert, dass die erwartete Rendite einer Risikobewältigungsmaßnahme oder Investition über dem risikoabhängigen Kapitalkostensatz liegt. Für die Unternehmenssteuerung müssen geeignete Erfolgsgrößen, sogenannte Performancemaße, definiert werden. Diese ermöglichen es, Ertrag und Risiko gegeneinander abzuwägen.

Vorwiegendes Ziel des Risiko- & Chancenmanagements ist eine risikooptimale Unternehmensposition, welche sich durch die bestmögliche Beherrschung der vorhandenen Risiken und einem sinnvollen Verhältnis von Gesamtrisiko und vorhandenem Eigenkapital auszeichnet. Die dafür notwendigen Instrumente der Risikosteuerung (Vermeiden, Verringern, Teilen und Akzeptieren) adressieren im Allgemeinen strategische und finanzielle Risiken mit hoher Komplexität und Materialität.

Kernaufgabe des Risiko- & Chancenmanagements eines Unternehmens ist es somit, die für das Unternehmen bedeutenden **strategischen** und **finanziellen Risiken** sowie **Risiken in Bezug auf die Compliance auf einem sehr hohen Niveau** und mit direktem Bezug zu den Unternehmenszielen zu ermitteln, zu bewerten und entsprechende Maßnahmen einzuleiten, damit diese auf ein für das Unternehmen akzeptables Niveau reduziert werden.

4.3.2 Compliance-Management

Als Compliance wird das Einhalten rechtlicher Rahmenbedingungen durch ein Unternehmen und seine Mitarbeiter bezeichnet. Dabei können als rechtliche Rahmenbedingungen einerseits geltende Gesetze, andererseits aber auch Kodizes wie etwa der Österreichische Corporate Governance Kodex[10] verstanden werden. Folglich bezeichnet das Compliance-Management die Gesamtheit der im Unternehmen eingerichteten Maßnahmen und Prozesse, um Regelkonformität sicherzustellen

[10] Vorrangig dient der Österreichischen Corporate Governance Kodex der Bereitstellung eines Ordnungsrahmens für österreichische Aktiengesellschaften, in dem bestimmte Anforderungen an Leitung und Überwachung des Unternehmens angeführt sind. Der Kodex enthält sowohl international übliche Standards für gute Unternehmensführung, als auch entsprechende Regelungen des österreichischen Aktienrechts. Hauptsächlich soll dadurch das Vertrauen der Aktionäre gefördert werden. Neben der Schaffung von Transparenz, steht der Fokus auch auf ein besseres Zusammenwirken von Aufsichtsrat, Vorstand und Aktionären sowie die Orientierung langfristiger Wertschaffungen [www.corporate-governance.at].

[Institut für Interne Revision 2014, S. 38]. Seitens des Risikomanagements stellen Verstöße gegen entsprechende Normen Risiken dar, die größtenteils schwer bis gar nicht quantifizierbar sind. Unternehmen haben als Konsequenz von Compliance-Vergehen neben monetären Bestrafungen auch mit einem massiven Imageverlust zu rechnen [Vgl. Wengert & Schittenheim 2013, S.8].

Integration des Compliance-Managements in das Risiko- & Chancenmanagement

An dieser Stelle soll geklärt werden, inwieweit und ob eine Integration mit einem im Unternehmen bestehenden Risiko- & Chancenmanagement sinnvoll bzw. möglich ist. Dabei stellt sich zunächst die Frage, warum in den meisten Unternehmen eine separate Betrachtung der Compliance-Risiken durchgeführt wird.

Compliance-Risiken werden häufig separat betrachtet, weil es im Risiko- und Chancenmanagement einerseits nicht oder nicht ausreichend gewürdigt wurde und andererseits die Kategorie der rechtlichen Risiken primär auf vertragliche Verpflichtungen, Rechtsstreitigkeiten bzw. laufende Prozesse oder Ähnliches ausgerichtet ist. Andere Compliance-Themen wie zum Beispiel Datenschutz oder Wettbewerbsrecht werden in der Regel im Zuge den Risiko- & Chancenmanagements nicht ausreichend betrachtet.

Außerdem werden Compliance-Risiken oftmals von dem Rechtsbereich erhoben und nicht aus dem klassischen Risikomanagement gestartet. Das Compliance-Management braucht nicht zwangsläufig eine harte Quantifizierung der Risiken, sondern kann auch auf Basis einer qualitativen Einschätzung durchgeführt werden. Daraus resultiert auch ein wesentlicher Grund gegen die Integration. Im Gegensatz zum quantitativ geprägten Risiko- & Chancenmanagement, welches häufig im Finanzbereich beim Controlling angesiedelt ist, benötigt das Compliance-Management zum Zwecke der Compliance-Prävention zwar eine Priorisierung der Compliance-Gefahren, aber weniger eine exakte Quantifizierung. Ein Nachteil der Separierung der beiden RM-Funktionen ist die gegebenenfalls bestehende Methodenvielfalt bei der Beurteilung der Risiken. Diese erschwert die Vergleichbarkeit der Risiken und die Aggregation zu einem Gesamtbild. Des Weiteren bedeuten zwei getrennte Risikobeurteilungen bis zu einem gewissen Grad Doppelarbeiten, die sich Unternehmen bei einer Integration sparen könnten.

Jedes Unternehmen sollte entsprechend der Vor- und Nachteile individuell abwägen, ob eine Integration des Compliance-Managements im Risiko- & Chancenmanagement sinnvoll ist. Laut Ekkenga & Kramer ist es jedoch vor allem bei der ersten Annäherung an das Compliance-Thema sinnvoll, vorerst eine separate Risikobeurteilung durch das Compliance-Management durchzuführen. Die lenkt besondere Aufmerksamkeit auf das Thema und ist für die Herausbildung einer Compliance-Kultur innerhalb des Unternehmens sehr hilfreich. Auf lange Sicht sollte jedoch eine Integration angestrebt werden, um Methodenvielfalt und Doppelarbeiten zu vermeiden [Ekkenga & Kramer 2011, S. 129].

4.3.3 Risiken im Risiko- & Compliancemanagement

Aus den vorigen Erläuterungen lassen sich nun folgende Risiken mit dem Risiko- & Chancenmanagement adressieren:

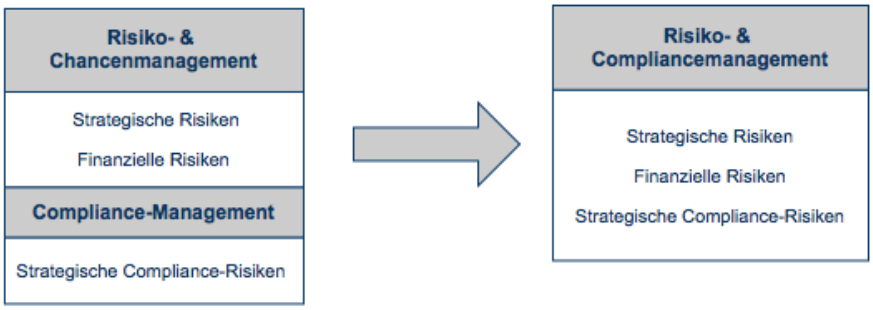


Abbildung 20: Risiken im Risiko- & Compliancemanagement

4.4 Third Line of Defense: Interne Revision

Die offizielle Übersetzung der originalen Begriffsbestimmung des Institute of Internal Auditors (IIA) lautet:

> *„Die Interne Revision erbringt unabhängige und objektive Prüfungs- und Beratungsdienstleistungen, welche darauf ausgerichtet sind, Mehrwerte zu schaffen und die Geschäftsprozesse zu verbessern. Sie unterstützt die Organisation bei der Erreichung ihrer Ziele, indem sie mit einem systematischen und zielgerichteten Ansatz die Effektivität des Risikomanagements, der Kontrollen und der Führungs- und Überwachungsprozesse bewertet und diese verbessern hilft.“*

Die Interne Revision ist nach dieser Definition für die Bewertung und die Verbesserung der Effektivität des Risikomanagements im Unternehmen verantwortlich. Als Bestandteil des Internen Kontrollsystems des Unternehmens hat die Interne Revision u.a. die Aufgabe, Mängel festzustellen und geeignete Verbesserungsmaßnahmen zu empfehlen sowie deren Umsetzung zu überwachen.

Die Aufgaben der Internen Revision erstrecken sich dabei von Ergebnisprüfungen und Einzelfallprüfungen über die Verfahrensprüfungen und Systemprüfungen der Funktionsfähigkeit des Überwachungssystems bis hin zur Prüfung der Unternehmensleitung. Demnach ist die Interne Revision ein integraler und unverzichtbarer Bestandteil der Führungsfunktion eines Unternehmens und fungiert zugleich als Sicherheitsnetz der Unternehmensleitung und des Aufsichtsrates.

Die folgende Auflistung zeigt eine Reihe von Aktivitäten, welche in der Literatur zwar oft der Internen Revision zugeschrieben, jedoch laut dem IIA Position Paper „The Role of Internal Auditing in Enterprisewide Risk Management" vom Jänner 2009 deutlich abgegrenzt werden und grundsätzlich eine Unterscheidung zwischen Hauptaufgaben, weiteren Aktivitäten und nicht empfohlenen Aufgaben vorgenommen wird [Vgl. Sommer 2010, S. 135]:

- **Hauptaufgaben:** Die primäre Aufgabe der internen Revision in Bezug auf das Risikomanagement besteht hauptsächlich in der Erbringung von Assurance-Dienstleistungen.
    - Assurance bezüglich des Risikomanagementprozesses
    - Assurance bezüglich der korrekten Evaluation von Risiken
    - Beurteilung der Risikomanagementprozesse
    - Beurteilungen der Berichterstattung über Hauptrisiken
    - Review der Handhabung der Hauptrisiken

- **Weitere Aktivitäten:** Die interne Revision kann neben den Prüfungs- auch Beratungsdienstleistungen im Bereich Risikomanagement erbringen.
    - Unterstützung bei der Identifikation und Bewertung von Risiken
    - Coaching des Managements betreffend der Handhabung von Risiken
    - Koordination der Risikomanagementaktivitäten
    - Konsolidierung der Berichterstattung über Risiken
    - Entwicklung und Aufrechterhaltung des Risikomanagements-Frameworks

- **Nicht empfohlene Aufgaben:** Diese Aufgaben obliegen der Unternehmensleitung bzw. des Linienmanagements und beeinträchtigen die Unabhängigkeit und Objektivität der Internen Revision.
    - Festlegen der Risikobereitschaft des Unternehmens
    - Entscheidung über die Einführung eines Risikomanagements
    - Entscheidungen hinsichtlich Maßnahmen zur Risikohandhabung
    - Implementierung solcher Maßnahmen
    - Übernahme der Verantwortung für das Risikomanagement

Zusammenfassend ist die Interne Revision somit eine vom Tagesgeschäft unabhängige, objektive Prüfungs- und Beratungsaktivität in einem Unternehmen und unterstützt dieses bei der Erreichung seiner Ziele im Wege eines systematischen und disziplinierten Ansatzes der Bewertung und Verbesserung der Effektivität von Risikomanagement bzw. internem Kontrollumfeld. Des Weiteren unterstützt die Interne Revision die Geschäftsführung in ihrer Kontroll-, Steuerungs- und Lenkungsfunktion im Wege der Durchführung unabhängiger, interner Prüfungsmandate und ist normalerweise direkt der Geschäftsführung des Unternehmens unterstellt.

Demnach adressiert die interne Revision jene Risiken, welche aus der Uneffizienz diverser Abläufe bzw. den Nichteinhalten von Vorgaben seitens des rPM und R-&CM resultieren. Im Weiteren werden diese Risiken als **Effektivitätsrisiken** bezeichnet.

4.5 Risikokategorisierung und Abgrenzung der adressierten Risiken im 3LoD-Modell

Abbildung 21 zeigt eine Erweiterung der Risikokategorisierung aus Kapitel 2. Hierbei werden alle Risiken angeführt, welche in den vorigen Kapiteln aus den Zielen der jeweiligen RM-Funktionen abgeleitet wurden.

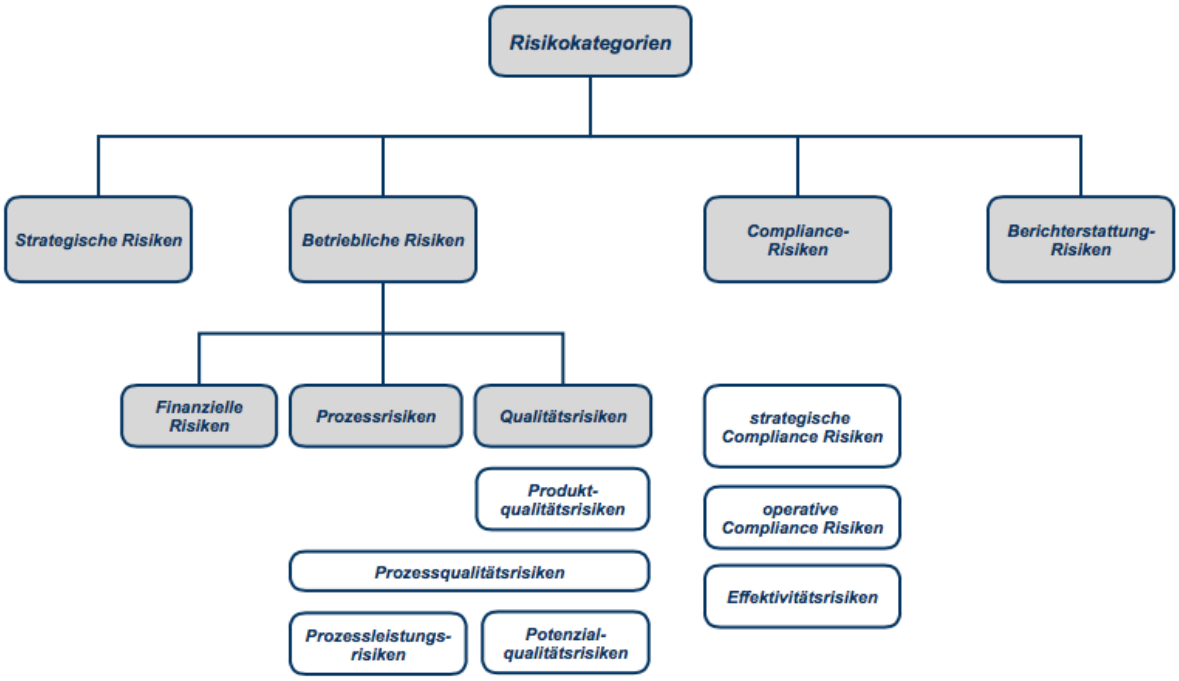


Abbildung 21: Risikokategorisierung II

In einem letzten Schritt können nun, unter Heranziehen der Risikokategorisierung aus Abbildung 21, alle Risiken des 3LoD-Modells eingeordnet werden. Dadurch kann aufgezeigt werden, welchen Risiken in welchen Unternehmensbereichen durch welche RM-Funktionen begegnet werden.

Dabei ist das **risikobasierte Prozessmanagement** im Zuge des Tagesgeschäftes für jene Risiken verantwortlich, welche im Allgemeinen durch Kontrollmaßnahmen im Prozessmanagement, Qualitätsmanagement und internen Kontrollsystem zu bewältigen sind.

Im Gegensatz dazu ist das **Risiko- & Compliancemanagement** für die Bewältigung komplexerer Risiken verantwortlich. Durch geeignete Steuerungsmaßnahmen werden im Risiko- & Chancenmanagement vorwiegend strategische und finanzielle Risiken adressiert, wohingegen das Compliance-Management Compliance-Risiken auf einem sehr hohen Niveau begegnet.

Im Zuge der **Internen Revision** werden jene Risiken behandelt, welche aus der Bedrohung der Regelkonformität im Unternehmen resultieren. Demnach ist die Interne Revision dafür verantwortlich, ob die vorgesehenen Kontrollmaßnahmen des risikobasierten Prozessmanagements bzw. Steuerungsmaßnahmen des Risiko- & Chancenmanagements auch eingehalten werden. Von zentraler Bedeutung ist dabei die Durchführung unabhängiger, interner Prüfungsmandate und Berichterstattung an die Geschäftsführung und den Prüfungsausschuss.

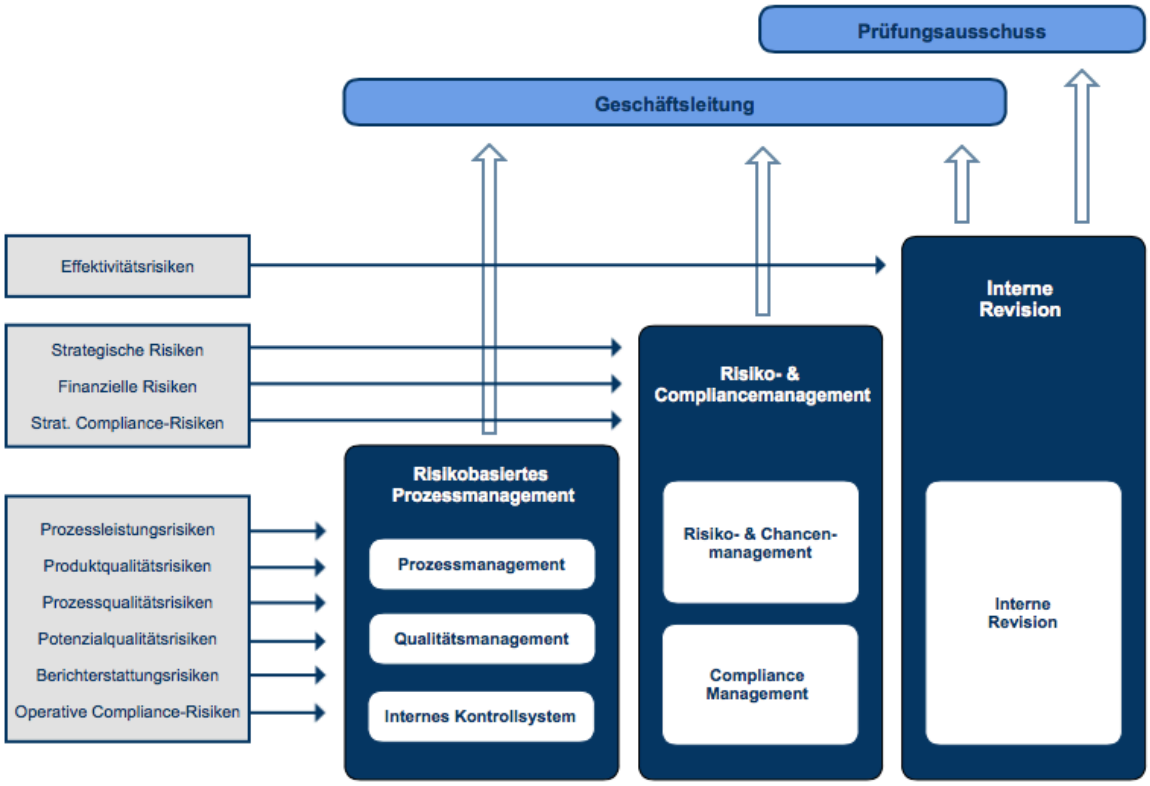


Abbildung 22: Risikoabgrenzung im unternehmensweiten Risikomanagement

Kapitel 5

Entwicklung eines Reifegradmodells für das unternehmens-weite RM

5.1 Grundlegende Vorgehensweise

Abbildung 23 zeigt die grundlegende Vorgehensweise zur Entwicklung eines Reifegradmodells für das unternehmensweite RMS.

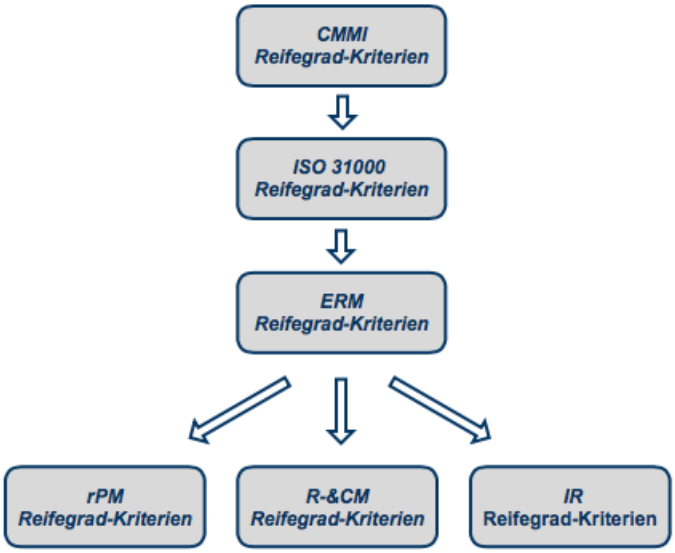


Abbildung 23: Entwicklung eines RG-Modells für das unternehmensweite RM

Den Ausgangspunkt stellen die Kriterien der Reifegrade des CMMI dar, welche durch Heranziehen der ISO 31000-Inhalte eine Ableitung der entsprechenden unternehmensweiten ERM-Reifegrad-Kriterien ermöglichen. Anschließend werden die einzelnen ERM-Reifegrad-Kriterien für das risikobasierte Prozessmanagement, das Risiko- & Compliancemanagement und die Interne Revision konkretisiert.

Ableiten der Reifegrad-Kriterien für das unternehmensweite Risikomanagement

Für die Ableitung der einzelnen ERM-Reifegrad-Kriterien sind drei Schritte zu durchlaufen, welche in der folgenden Tabelle für die Reifegrade 2 bis 4 dargestellt sind:

<table>
<tr><th></th><th>1. Schritt</th><th>2. Schritt</th><th>3. Schritt</th></tr>
<tr><th></th><th>CMMI
Reifegrad-Kriterium</th><th>ISO 31000
Reifegrad-Kriterium</th><th>ERM
Reifegrad-Kriterien</th></tr>
<tr><td>RG 2</td><td rowspan="2">Arbeitsabläufe werden entsprechend der unternehmensweiten Leitlinien geplant und haben eine grundlegende Infrastruktur zu deren Umsetzung.</td><td rowspan="2">Der Einsatz von Instrumenten und Methoden ermöglicht sowohl eine strukturierte Risikobeurteilung als auch daraus abgeleitete strukturierte Risikobewältigungsmaßnahmen.</td><td>Strukturierte Risikobeurteilung</td></tr>
<tr><td>Strukturierte Risikobewältigung</td></tr>
<tr><td rowspan="2">RG 3</td><td rowspan="2">Arbeitsabläufe werden in Form von Normen, Verfahren und Methoden genau beschrieben bzw. ausführlich dokumentiert.

Die Leistung von ausgewählten Teilprozessen wird mithilfe statistischer und quantitativer Techniken gesteuert.</td><td rowspan="2">In einem Risikobewältigungsplan wird ausführlich dokumentiert, wie die ausgewählten Maßnahmen zur Risikobewältigung umgesetzt werden.

Quantitative Verfahren der Risikobeurteilung ermöglichen aussagekräftige Werte zur Leistungssteuerung.</td><td>Quantitative Leistungsbeurteilung</td></tr>
<tr><td>Ausführliche Risikodokumentation</td></tr>
<tr><td>RG 4</td><td>Schwerpunkt liegt auf der Gesamtleistung der Organisation, wobei Daten aus mehreren Projekten herangezogen werden.</td><td>Relevante Informationen aus dem Risikomanagement stehen auf entsprechenden Ebenen der Organisation zur rechten Zeit zur Verfügung.</td><td>Integrierter Ansatz</td></tr>
</table>

Tabelle 4: Ableiten der ERM-Reifegrad-Kriterien

1. Schritt: Zu Beginn werden die wesentlichen Merkmale eines jeden CMMI-Reifegrades (Kapitel 2.2.2) zusammengefasst und der verdichtete Informationsgehalt durch ein CMMI-Reifegrad-Kriterium ausformuliert. Da jedes Unternehmen Reifegrad 1 automatisch erreicht, werden die Reifegrad-Kriterien ausschließlich für die Reifegrade 2 bis 4 hergeleitet.

2. Schritt: Unter Heranziehen der Inhalte der ISO 31000, werden die CMMI-Reifegrad-Kriterien um die Risikobetrachtung ergänzt und so die entsprechenden ISO 31000- Reifegrad-Kriterien abgeleitet. Dabei wird die ISO 31000 dem COSO II-Rahmenwerk vorgezogen, da COSO II Risikomanagement schon per Definition (Kapitel 3.2) vorwiegend als Prozess ansieht, wohingegen ISO 31000 den Schwerpunkt sowohl auf den RM-Prozess als auch auf den RM-Rahmen legt. Beide folgen dabei einer PDCA-Logik im Sinne eines Deming-Kreises.

3. Schritt: Abschließend werden aus den ISO 31000-Reifegrad-Kriterien heraus die ERM-Reifegrad-Kriterien für das unternehmensweite Risikomanagement definiert.

Beim CMMI-Reifegrad-Modell erreicht jedes Unternehmen automatisch Reifegrad 1. Diesem Ansatz folgend, werden ausschließlich ERM-Reifegrad-Kriterien für die Reifegrade 2 bis 3 abgeleitet. An dieser Stelle sei darauf hingewiesen, dass die ursprüngliche Anzahl von fünf Reifegraden im CMMI aus Gründen der Vereinfachung auf vier Reifegrade reduziert wurde. Grund dafür ist die hohe Komplexität des CMMI, welches auf das gesamte Unternehmen, also auf alle Abteilungen ausgerichtet ist und demnach das RM nur beiläufig miteinbezieht.

ERM-Reifegrad-Kriterien für Reifegrad 2: Strukturierte Risikobeurteilung und -bewältigung

Im Zuge einer **strukturierten Risikobeurteilung und -bewältigung** geht es vor allem darum, mit geeigneten Methoden die Risiken im Unternehmen rechtzeitig zu identifizieren, zu bewerten und anschließend entsprechende Bewältigungsmaßnahmen abzuleiten. Dafür ist es notwendig zu wissen, wo Risiken auftreten und wie diesen Risiken begegnet werden kann. Risikobewältigungsmaßnahmen werden im Folgenden beim risikobasierten Prozessmanagement als Kontrollmaßnahmen, beim Risiko- & Chancenmanagement als Steuerungsmaßnahmen und bei der Internen Revision als Prüfmaßnahmen bezeichnet und werden folgendermaßen kategorisiert:

Risikobewältigungsmaßnahmen		
Manuelle und automatische **Kontrollmaßnahmen** finden im rPM Anwendung.	**Steuerungsmaßnahmen** sind eindeutig dem R- & CM zuzuschreiben (Vermeiden, Verringern, Teilen und Akzeptieren von Risiken)	**Prüfmaßnahmen** sind eindeutig der IR zuzuschreiben, welche das Einhalten interner Abläufe überprüfen.

Tabelle 5: Risikobewältigungsmaßnahmen im unternehmensweiten RMS

ERM-Reifegrad-Kriterien für Reifegrad 3: Quantitative Leistungssteuerung und ausführliche Risikodokumentation

Bei der **quantitativen Leistungssteuerung** spielen einerseits im risikobasierten Prozessmanagement und der Internen Revision sogenannte Risikoindikatoren und andererseits im strategischen Risiko- & Compliancemanagement die Quantifizierung von Risiken durch entsprechende Risikomaße eine bedeutende Rolle.

Risikoindikatoren sind Kennzahlen, die sich auf Geschäftsprozesse beziehen und in der Lage sind, Veränderungen im Risikoprofil dieser Geschäftsprozesse vorherzusehen [www.risknet.de].

Demnach stellt ein Risikoindikator eine rationale und quantitative Kennzahl eines bestimmten Risikos zu einer bestimmten Zeit dar. Dafür werden normalerweise kritische Werte (Schwellenwerte) vorgegeben, die in Verbindung mit einem Ampelsystem als Frühwarnsystem dienen können. Abbildung 24 zeigt ein Beispiel eines solchen Ampelsystems, bei dem die Werte der Indikatoren je nach Festlegung der Schwellenwerte in die drei mit den Phasen einer Ampel vergleichbaren Zonen unterteilt werden [Vgl. Romeike & Brink, S. 4].

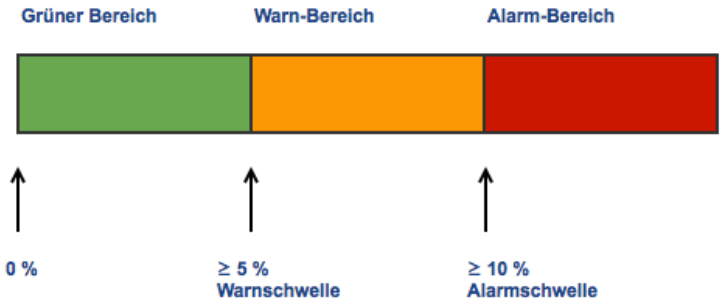


Abbildung 24: Schwellenwerte im Ampelsystem [Vgl. Romeike & Brink, S. 4]

- Bewegt sich ein Risikoindikator im grünen Bereich, so besteht kaum Gefahr und kein konkreter Handlungsbedarf. Dennoch sollten Indikatoren im grünen Bereich laufend beobachtet werden.
- Dagegen erfordern Indikatoren im gelben Bereich erste Untersuchungen, eine intensive Überwachung einzelner Aspekte und ggf. erste Anpassungen der Steuerungsmaßnahmen, um die Risikosituation nicht zu verschärfen (Warnschwelle).
- Risikoindikatoren, die sich im roten Bereich befinden verlangen unmittelbaren Handlungsbedarf (Warnschwelle).

Risikomaße wandeln Wahrscheinlichkeitsverteilungen von Risiken in einfach interpretierbare Zahlen um, wodurch sie einen Vergleich verschiedener Risiken mit unterschiedlichen Charakteristika, Verteilungsformen und -parametern ermöglichen. Das traditionelle Risikomaß der Kapitalmarkttheorie stellt die Varianz (Var(X)) bzw. die Standardabweichung (SD(X)) dar. Diese Volatilitätsmaße beschreiben das Ausmaß der Schwankungen einer risikobehafteten Größe um die mittlere Entwicklung, den sogenannten Erwartungswert (E(X)) einer Zufallsvariable X. Im Gegensatz dazu berücksichtigen Shortfall-Maße, wie zum Beispiel der Value at Risk (VaR(X)) oder der Expected Shortfall (ES(X)) lediglich die negativen Abweichungen von einem erwarteten Wert [Romeike & Hager 2009, S. 147].

An dieser Stelle sollen nicht sämtliche Risikomaße aufgezählt werden, sondern stellevertretend dafür der Value at Risk genauer beschrieben werden, da dieses Risikomaß in der Praxis am häufigsten Anwendung findet. Der Value at Risk ist als diejenige Schadenhöhe definiert, die innerhalb einer bestimmten Zeit-Periode T mit einer festgelegten Wahrscheinlichkeit (Konfidenzniveau 1-α) nicht überschritten wird [Vgl. Stephan 2006, S. 176]. Formal gesehen ist der Value at Risk die Differenz zwischen dem Erwartungswert und dem Quantil einer Verteilung. Dabei gibt das x %-Quantil zu einer Verteilung jenen Schwellwert an, bis zu den x % aller möglichen Werte liegen (Abbildung 25). Bei einer Normalverteilung mit Erwartungswert E(X) und Standardabweichung SD(X) berechnet sich der VaR wie folgt [Romeike & Hager, S.148]:

$$VaR_{1-\alpha}(X) = -(E(X) + q_\alpha * SD(X)$$

Dabei ist q_α das aus einer Tabelle ablesbare Quantil der Normalverteilung zum Konfidenzniveau 1-α. Bezieht sich der VaR nicht auf einen Wert, sondern z.B. auf einen Cashflow, spricht man von einem Cashflow at Risk, was jedoch das gleiche Risikomaß meint. Ergänzend sei erwähnt, dass der VaR nicht nur bei Normalverteilungen, sondern für beliebige Verteilungen berechenbar ist [Gleissner 2011, S. 138].

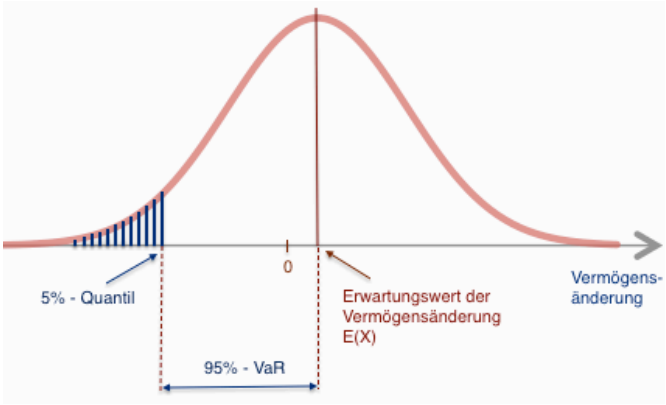


Abbildung 25: VaR mit Konfidenzniveau 95% [Vgl. Stephan 2006, S. 177]

Im Zuge einer **ausführlichen Dokumentation** ist es notwendig entsprechende Einzelheiten zu den Risiken bzw. deren Bewältigungsmaßnahmen in Form von Risikoinventaren bereitzustellen. Im Allgemeinen liefert ein Risikoinventar in einer übersichtlichen Form Informationen über die Risikosituation eines Unternehmens. Dabei kann es unter anderem folgende Punkte enthalten [Denk 2008, S. 119]:

- Alle Einzelrisiken, beispielsweise gegliedert nach organisatorischen Funktionsbereichen,
- qualitative oder quantitative Bewertungen der Risiken,
- Toleranzgrenzen bei Risikoindikatoren,
- Informationen zu Risikobewältigungsmaßnahmen
- Verantwortungen für die Umsetzung der Risikobewältigungsmaßnahmen,
- Termine für die Umsetzung der Risikobewältigungsmaßnahmen,
- Beurteilung der Wirksamkeit der bestehenden Risikobewältigungsmaßnahmen.

In der vorliegenden Arbeit wird aus übersichtlichen Gründen folgende Unterteilung bezüglich der Dokumentation von Risiken getroffen, auf welche in den folgenden Kapiteln näher eingegangen wird:

Risiko-Kontrollinventar	Risiko-Steuerungsinventar	Risiko-Prüfinventar
Dokumentation der wesentlichen Risikoinformationen im Zuge des risikoorientierten Prozessmanagements.	Dokumentation der wesentlichen Risikoinformationen innerhalb des Risiko- & Compliance-management.	Dokumentation der wesentlichen Risikoinformationen innerhalb der Internen Revision.

Tabelle 6: Dokumentation der wichtigsten Risikoinformationen

ERM-Reifegrad-Kriterien für Reifegrad 4: Integrierter Ansatz

Für den **integrierten Ansatz** ist vor allem der Begriff des „Integrierten Managementsystems“ von zentraler Bedeutung. Im Allgemeinen wird unter Integriertem Management-System jene Vorgehensweise verstanden, bei der Anforderungen aus verschiedenen Bereichen (z.B. Gesundheit, Sicherheit, Umwelt, Qualität, ...) in einer einheitlichen Struktur zusammengefasst werden. Durch Nutzung von Synergien und die Bündelung von Ressourcen ist, im Vergleich zu einzelnen bzw. isolierten Managementsystemen, ein schlankeres, effizienteres Management möglich [VDI 4060, Blatt 2].

5.2 Reifegrade des risikobasierten Prozessmanagements

In diesem Kapitel werden die ERM-Kriterien für das risikobasierte Prozessmanagement konkretisiert. Ausgangspunkt dafür sind nicht die RM-Funktionen innerhalb der 1st-LoD, sondern die Risiken selbst, denen es im Zuge des Tagesgeschäftes zu begegnen gilt (Abbildung 26). Dadurch sind die entsprechenden Kriterien unabhängig davon, aus welchen der RM-Funktionen heraus die 1st-LoD aufgebaut ist. So ist es beispielsweise nicht ausschlaggebend für einen Reifegrad, ob Risiken im Qualitätsmanagement oder Prozessmanagement adressiert werden, sondern dass diese Risiken adressiert werden.

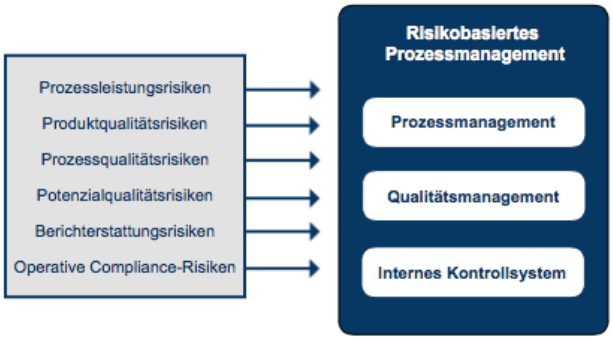


Abbildung 26: Risiken im risikobasierten Prozessmanagement

5.2.1 Strukturierte Risikobeurteilung und -bewältigung beim rPM

Beim **Prozessmanagement** bilden die Geschäftsprozesse selbst den Ausgangspunkt für die Risikobeurteilung. Hierbei soll eine Modellierung der wesentlichen Geschäftsprozesse ermöglichen, potentielle Risiken entlang der Prozesskette zu visualisieren. Demnach stellt das Prozessmanagement Prozesse in das Zentrum der Risikobetrachtung um Ursache, Entstehungsorte und Auswirkung der Prozessleistungsrisiken zu analysieren [Rieke & Winkelmann 2008, S. 347]. Um Verbesserungspotenziale von Geschäftsprozessen zu erheben und anschließend zu realisieren, folgt das Prozessmanagement im Allgemeinen einem bestimmten Ablauf, welcher im Folgendem, stellvertretend durch die 4-Schritte-Methode nach Wagner, dargestellt ist [Wagner & Käfer 2013, S. 55]:

- Schritt I: Identifizierung und Abgrenzung
- Schritt II: Analyse Ist-Prozesse
- Schritt III: Konzeption Soll-Prozesse
- Schritt IV: Realisierung Verbesserungspotential (Umsetzen der Soll-Prozesse)

Ziel dieses Ablaufes ist es demnach, mögliche Gefahren im bestehenden Prozessablauf zu identifizieren (Analyse Ist-Prozesse), Maßnahmen für deren Vermeidung zu erarbeiten (Konzeption Soll-Prozess) und anschließend diese Maßnahmen im Unternehmen umzusetzen. Streng genommen entspricht dieser Ablauf dem der Risikobeurteilung und -bewältigung.

In der Praxis findet eine Reihe verschiedener Methoden Anwendung, um Risiken im Zuge des Prozessmanagements zu identifizieren bzw. anschließend zu bewerten. Tabelle 7 zeigt häufig angewendete Methoden gemäß ihrer Eignung zur Identifikation und Bewertung von Risiken [Vgl Müllner et al. 2013, S. 344].

Methode	Risikoidentifikation	Risikobewertung		
		Auswirkung	Wahrscheinlichkeit	Risikohöhe
Brainstorming	+++	+	+	
FMEA	+++	++	++	+
Szenarioanalysen	+++	+++	++	++

Tabelle 7: Häufig angewendete Methoden im Prozessmanagement [Müllner et al. 2013, S. 344]

Im Zuge von sogenannten **Brainstorming**-Workshops identifizieren die involvierten Personen die möglichen Problemfelder des Geschäftsprozesses und dessen Betrachtungsobjekte. Da Brainstorming zu den Kreativtechniken zählt, eignet es sich sehr gut zur Identifikation von möglichen Risiken, jedoch weniger zur Bewertung derselben.

Die **FMEA (Failure Mode and Effects Analysis)** zerlegt die Gesamtsysteme in ihre Teilsysteme und Prozesse, je nach erforderlicher Bearbeitungstiefe, ebenfalls in ihre Einzelteile. Anschließend ermittelt die FMEA detailliert die Funktionen der Einzelteile und sucht nach möglichen Fehlerfunktionen und ihren Ursachen, welche die Funktionsfähigkeit der Einzelteile und damit des Gesamtsystems beeinträchtigen können. Die Fehlfunktionen werden mit der Risikoprioritätszahl (RPZ) gewichtet [Vgl. Müllner et al. 2013, S. 345].

Szenarioanalysen beschreiben im Allgemeinen die zukünftige Entwicklung eines Prognosegegenstandes bei alternativen Rahmenbedingungen, um kausale Zusammenhänge und Entscheidungspunkte herauszuarbeiten. Ein Szenario ist nichts anderes als in die Zukunft geschriebene Geschichte, wobei man aus der Vergangenheit und der Gegenwart mögliche Zukunftsbilder generiert [Romeike & Hager 2009, S. 145].

Um Risiken in Unternehmen im Zuge eines **Qualitätsmanagements** zu begegnen, stellt vor allem, wie in Kapitel 4 beschrieben, die Einhaltung der Qualitätsanforderungen an Produkte, Prozesse und Potenziale den Mittelpunkt der Risikobetrachtung dar. Diese Anforderungen können im Unternehmen explizit durch folgende Hilfsmittel definiert sein [Vgl. Schneider et al. S 21]:

- Arbeits- und Prüfanweisungen
- Checklisten
- Formulare
- Interne Richtlinien

Demnach kann das Vorhandensein und die Einhaltung entsprechender Qualitätsanforderungen im Unternehmen als Bewältigung von Qualitätsrisiken interpretiert werden. Aus der Sicht der Risikobeurteilung ist vor allem die im Kapitel 4.2.2 angesprochene Kundennähe ausschlaggebend. So wird die Qualität der Produkte und Dienstleistungen letztendlich durch die Ansprüche der Kunden und des Marktes bestimmt. Aus der Sicht der Risikobeurteilung ist also das Wissen über die jeweiligen Kundenansprüche von großer Bedeutung.

Gängige Methoden des Qualitätsmanagements, welche zur Aufdeckung potentieller Gefahren bei der Einhaltung von Qualitätsanforderungen Verwendung finden, sind denen des Prozessmanagements sehr ähnlich bzw. häufig die selben. So wird im Zuge des Qualitätsmanagements die FMEA dafür eingesetzt, um frühzeitig mögliche Fehlerquellen bei der Einhaltung von Qualitätsanforderungen zu entdecken. Von einer Abgrenzung soll im Zuge dieser Arbeit jedoch abgesehen und an dieser Stelle auf Tabelle 7 verwiesen werden, welche Beispiele für jene Methoden auflistet, die sowohl im Prozess-, als auch im Qualitätsmanagement eingesetzt werden.

Aus der Sicht des Internen **Kontrollsystems mit engem Fokus** stellen die einzelnen Positionen des Jahresabschlusses den Ausgangspunkt der Risikobeurteilung dar. Dabei werden entsprechende Faktoren beurteilt, um jene Unternehmensteile auszuwählen, welche einen wesentlichen Beitrag zur Erreichung der Ziele der finanziellen Berichterstattung erbringen. Solche Kriterien können beispielsweise sein:

- Das Transaktionsvolumen,
- die Komplexität eines Rechnungslegungsstandard,
- der prozentuale Beitrag der Unternehmensteile zum Jahresabschluss.

Nach der qualitativen oder quantitativen Bewertung der Einzelrisiken anhand möglicher Auswirkungen auf den Jahresabschluss, werden entsprechende Kontrollmaßnahmen zur deren Eliminierung oder Reduzierung definiert [Hunziger 2011, S. 4].

Diese Kontrollmaßnahmen können entweder manueller oder automatischer Natur sein. Manuelle Kontrollen beruhen hauptsächlich auf der manuellen Ausführung durch eine oder mehrere Personen. Automatische (systembasierte) Kontrollen vertrauen hingegen bei der Ausführung hauptsächlich auf speziell programmierte Anwendungen oder IT-Systeme, welche ohne manuelle Interaktion oder Entscheidungsfindung bestimmte Transaktionen blockieren können. Ebenso gibt es systembasierte, manuelle Kontrollen wie z.B. den Vergleich zweier Komponenten, wobei die Auswahl der zum Vergleich stehenden Komponenten vom System bestimmt wurde. Die Qualität der manuellen Kontrolle hängt dabei von der Verlässlichkeit des Systems ab [Bungartz 2011, S. 58]. Bei der Auswahl der Kontrollmaßnahmen sind vor allem folgende Prinzipien des Internen Kontrollsystems von Bedeutung [http://kmu.pwc.at/#!wachsen/was-ist-iks-und-wozu]:

- **Prinzip der Transparenz:** Für jeden Prozess muss es eine Ablaufbeschreibung geben. So kann auch ein Außenstehender beurteilen, ob ein Prozess ordnungsgemäß abläuft.
- **Prinzip der vier Augen:** Eine einzelne Person darf nicht alleine für einen Prozess verantwortlich sein und auch nicht alleine über das Vermögen des Unternehmens verfügen.
- **Prinzip der Funktionstrennung:** Im Unternehmen müssen Auftragserfüllung und Auftragskontrolle (Soll-Ist-Vergleich) getrennt sein.
- **Prinzip der Mindestanforderung:** Für Mitarbeiter sollen nur diejenigen Informationen verfügbar sein, die sie für ihre Arbeit brauchen – inklusive entsprechender Sicherungsmaßnahmen bei IT-Systemen.

Ausformulieren des rPM-Kriteriums für Reifegrad 2

Um Reifegrad 2 im risikobasierten Prozessmanagement zu erreichen, ist eine strukturierte Beurteilung und Bewältigung aller in der 1st-LoD adressierten Risiken notwendig (Abbildung 26). Den Ausgangspunkt dafür stellt die Modellierung der wesentlichen Geschäftsprozesse dar. Anhand dieser modellierten Prozesse lassen sich die Prozessleistungsrisiken, Qualitätsrisiken, Berichterstattungsrisiken und operativen Compliance-Risiken ableiten. Dafür werden unter Heranziehen der Anforderungen an Qualität, Leistung, finanzielle Berichterstattung und Compliance die einzelnen Risiken entlang der Prozesskette identifiziert und bewertet. Im Zuge der strukturierten Risikobewältigung werden manuelle und/oder automatische Kontrollmaßnahmen zur Vermeidung bzw. Verringerung der identifizierten Risiken bestimmt.

rPM-Kriterium für Reifegrad 2
Basierend auf der **Modellierung der wesentlichen Geschäftsprozesse** werden durch die jeweiligen Anforderungen an Leistung, Qualität, finanzielle Berichterstattung und Compliance die entsprechende **Prozessleistung-, Qualitäts-, Berichterstattungs- und Compliance-Risiken** abgeleitet und bewertet. Zur Vermeidung bzw. Verringerung der Risiken werden geeignete **manuelle oder automatische Kontrollmaßnahmen** bestimmt.

5.2.2 Quantitative Leistungssteuerung und ausführliche Dokumentation im rPM

Bei der **quantitativen Leistungssteuerung** im risikobasierten Prozessmanagement spielen vor allem Risikoindikatoren in Verbindung mit einem sogenannten Ampelsystem eine bedeutende Rolle.

Im Prozessmanagement fordert die **ausführliche Dokumentation** eine entsprechende Modellierung der Geschäftsprozesse unter Heranziehen gängiger Modellierungssprachen (UML, ARIS, etc.). Hauptaufgabe des Qualitätsmanagement im Sinne einer **ausführlichen Dokumentation** liegt darin, dass alle qualitativen Anforderungen an Produkte und Prozesse explizit definiert durch beispielsweise folgende Dokumente vorliegen:

- Arbeitsanweisung,
- Interne Richtlinie, etc.

Seitens des Internen Kontrollsystems werden im Zuge einer **ausführlichen Dokumentation** die wesentlichen Informationen zu den im Internen Kontrollsystem adressierten Risiken in einem sogenannten Risiko-Kontrollinventar gesammelt. Dabei stellen die folgenden Punkte den Mindeststand der Dokumentation dar:

- Identifizierte Risiken und entsprechende Kontrollmaßnahmen zu deren Bewältigung
- Verantwortlichkeiten für die Kontrollmaßnahmen
- Eine detaillierte Beschreibung der Sollprozesse und entsprechende Informationen zu deren Umsetzung im Unternehmen.

Ausformulierung des RPM-Kriteriums für Reifegrad 2

Zusammenfassend ist die quantitative Leistungssteigerung des risikobasierten Prozessmanagements durch den Einsatz von Risikoindikatoren gekennzeichnet.

Die ausführliche Dokumentation des risikobasierten Prozessmanagements verlangt vor allem eine präzise und dokumentierte Modellierung der wesentlichen Geschäftsprozesse. Dafür werden im Unternehmen gängige Modellierungssprachen eingesetzt (z.B.: UML, ARIS, etc.). Des Weiteren sind in einem Risiko-Kontrollinventar die wichtigsten Informationen zu den Kontrollmaßnahmen vorhanden.

rPM-Kriterium für Reifegrad 3
Risikoindikatoren dienen in Verbindung mit einem Ampelsystem als Frühwarnsystem. Unter Verwendung gängiger **Modellierungssprachen** werden die wesentlichen Geschäftsprozesse präzise modelliert. Ein ausführliches **Risiko-Kontrollinventar** beinhaltet alle identifizierten Risiken und die entsprechenden Kontrollmaßnahmen zu deren Bewältigung sowie die dafür vorgesehenen Verantwortlichen.

5.2.3 Integrierter Ansatz im rPM

Im Sinne eines integrierten Management-Systems werden entsprechende Synergien zu anderen Management-Systemen genutzt. Besonders von Bedeutung ist in diesem Zusammenhang jenes Synergiepotenzial, welches sich aus der gemeinsamen Nutzung einer IT-gestützten Plattform mit dem Risiko- & Compliancemanagement ergibt. Dadurch können gleiche Daten über Prozesse, Kennzahlen und relevante Risikoinformationen abgeglichen und ausgetauscht werden, wodurch Diskrepanzen und Doppelgleisigkeiten vermieden werden.

rPM-Kriterium für Reifegrad 4
Durch die gemeinsame Nutzung einer **IT-gestützten Plattform** können das risikobasierte Prozessmanagement und das Risiko- & Compliancemanagement gleiche Daten über Prozesse, Kennzahlen und relevante Risikoinformationen abgleichen bzw. austauschen und so Diskrepanzen und Doppelgleisigkeiten vermieden werden.

5.3 Reifegrade des Risiko- & Compliancemanagement

Analog zu Kapitel 5.2 stellen auch im Risiko- & Compliancemanagement die adressierten Risiken den Ausgangspunkt für die Konkretisierung der ERM-Kriterien dar (Abbildung 27). So sind die entsprechenden Kriterien dahingehend zu formulieren, dass nicht zwingendermaßen ein Compliance-Management für die Bewältigung von Compliance-Risiken im Unternehmen vorhanden sein muss, wenn diesen Risiken auch im Zuge einen entsprechend ausgebauten Risiko- & Chancenmanagements begegnet werden kann.

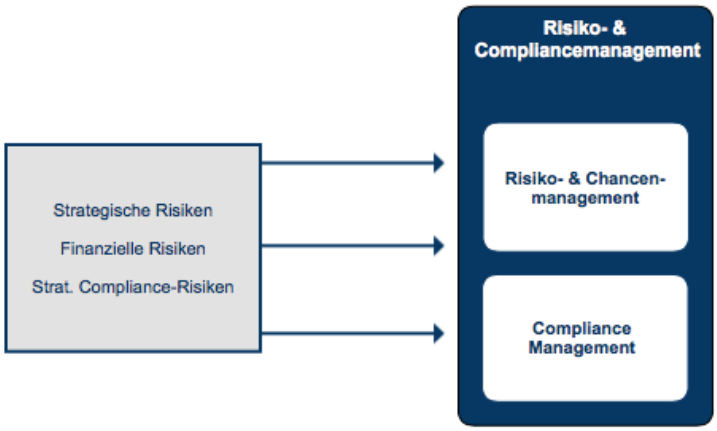


Abbildung 27: Risiken im Risiko- & Compliancemanagement

5.3.1 Strukturierte Risikobeurteilung und -bewältigung im R-&CM

Im Rahmen des **Risiko- & Chancenmanagements** werden im Zuge der strukturierten Risikobeurteilung die Unternehmensstrategie und die diese tragenden Erfolgspotenziale kritisch analysiert. Erfolgspotenziale eines Unternehmens sind Ressourcen und Fähigkeiten, die maßgeblich für zukünftige Erträge bzw. Cashflows verantwortlich sind. Einerseits können dies vom Kunden wahrnehmbare Wettbewerbsvorteile (z.B. Servicequalität) oder andererseits besondere interne Stärken im Vergleich zu den Wettbewerbern sein [Gleissner 2011, S. 72].

Stellvertretend für die Instrumente zur Identifizierung strategischer Risiken soll die sogenannte SWOT-Analyse näher beschrieben werden. Mit Hilfe dieses Verfahrens können aus der Markt-, Wettbewerbs- und Organisationsanalyse Stärken, Schwächen, Chancen und Risiken (SWOT = strengths, weaknesses, opportunities and threats) abgeleitet werden. Das Resultat ist eine genaue Bestandsaufnahme des gegenwärtigen Zustandes und liefert klare Erkenntnisse über [Romeike & Hager 2011, S. 125]:

- den Ist-Zustand der eigenen Organisation (Kernkompetenzen),
- die Zielgruppen (Zielgruppenfokus und -bedürfnisse),
- das Wettbewerbsumfeld (Positionierung, Leistungsumfang und Alleinstellungsmerkmale)
- die Aufstellung am Markt (Marktpräsenz).

Beim Compliance-Management geht es bei **der strukturierten Risikobeurteilung** darum, die relevanten Rechtsgebiete und die daraus erwachsenen spezifischen Anforderungen an das Unternehmen zu ermitteln. Dabei soll keine Vollerhebung aller gesetzlichen Vorschriften für ein Unternehmen vorgenommen werden, sondern die branchen- und unternehmensspezifischen Besonderheiten identifiziert und daraus entsprechende Compliance-Gefahren erkannt werden.

Für die gängigen Methoden, welche häufig für die Identifizierung von Compliance-Risiken herangezogen werden, soll stellvertretend die sogenannte PESTEL-Analyse erwähnt werden. Dabei handelt es sich um eine Analyse des makropolitischen Umfelds und dessen Einfluss auf das Unternehmen. PESTEL ist die Abkürzung für die betrachteten Themenfelder: Political, Econmical, Sociocultural, Technological, Environmental und Legal [Ekkenga & Kramer 2011, S. 121].

Bei der Risikobewertung von finanziellen, strategischen und Compliance-Risiken muss im Allgemeinen zwischen qualitativen und quantitativen Methoden unterschieden werden. Die strukturierte Risikobeurteilung geht jedoch ausschließlich von einer qualitativen Methode aus, da quantitative Methoden erst bei der quantitativen Leistungsmessung auf Reifegrad 3 Anwendung finden.

Im Zuge einer qualitativen Messung werden die Größen „Schadensausmaß“ und „Eintrittswahrscheinlichkeit“ über mit Adjektiven hinterlegten Skalen (Abbildung 28) beschrieben [Vgl. Brühwiler & Romeike 2010, S. 154]. Diese pragmatische Einteilung des Schadensausmaßes in „spürbar “, „bedeutend “ und „schwerwiegend“ orientiert sich dabei an der Gesamtbedeutung des Risikos für ein Unternehmen. Mit Hilfe dieser relativ einfachen Ausgestaltung der Risikoanalyse können die Risiken in einer qualitativen Risk-Map abgebildet werden und so jene für das Unternehmen signifikante Risiken abgeleitet werden (Abbildung 26) [Vgl. Brühwiler & Romeike 2010, S. 154].

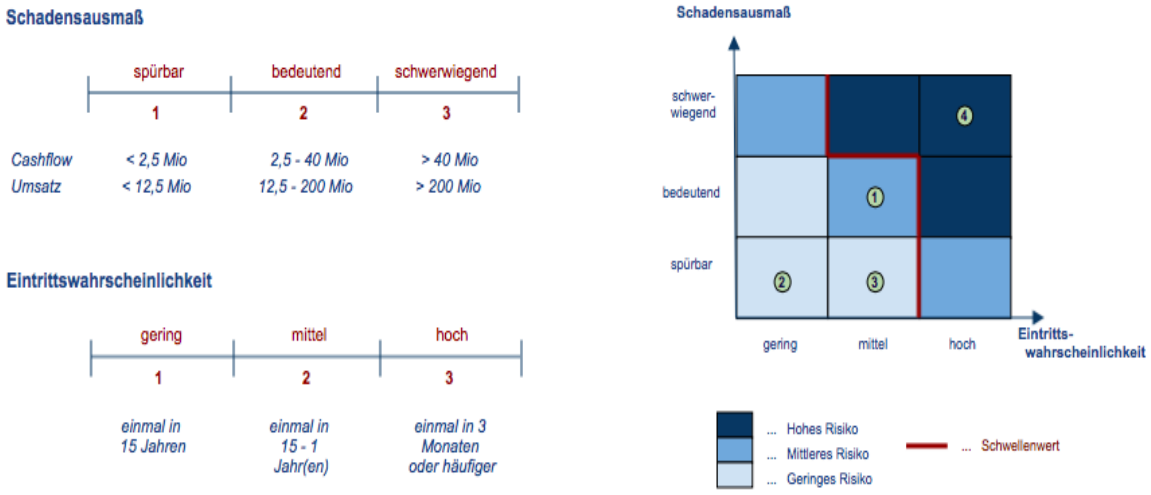


Abbildung 28: Wesentlichkeitsskalen und qualitatives Risikoportfolio [Vgl. Merz 2011, S. 27]

Die **strukturierte Risikobewältigung** sieht beim Risiko- & Compliancemanagement die im Zuge dieser Arbeit als Steuerungsmaßnahmen definierten Risikobewältigungsmaßnahmen der Vermeidung, Verringerung, Teilung oder Akzeptanz von Risiken vor. Jene Maßnahmen, die aus der Beurteilung von Compliance-Risiken abgeleitet werden können, haben vorwiegend präventiven Charakter, da es darum geht, Compliance-Verstöße in Zukunft zu verhindern und nicht bereits eingetretene Verfehlungen zu behandeln.

Ausformulierung des RPM-Kriteriums für Reifegrad 2

Voraussetzung für Reifegrad 2 ist die strukturierte Beurteilung und Bewältigung aller im Risiko- & Compliancemanagement adressierten Risiken. Demnach müssen auf Reifegrad 2 im Unternehmen Methoden zur Beurteilung und Bewältigung sowohl von finanziellen als auch strategischen und Compliance-Risiken vorhanden sein.

R-&CM-Kriterium für Reifegrad 2
Aus den **Bedrohungen** der für das Unternehmen wichtigen **Erfolgspotenziale** werden **strategische** und **finanzielle Risiken** identifiziert und bewertet. Die für das Unternehmen **relevanten Rechtsgebiete** sind bekannt und werden zur Identifizierung bzw. Bewertung der **Compliance-Risiken** herangezogen. Um Risiken zu Vermeiden, Verringern, Teilen oder Akzeptieren werden entsprechende **Steuerungsmaßnahmen** bestimmt.

5.3.2 Quantitative Leistungssteuerung und ausführliche Dokumentation im R-&CM

Im Zuge der **quantitativen Leistungsbeurteilung** finden im Risiko- & Chancenmanagement, neben Risikoindikatoren, vorwiegend Risikomaße Anwendung, welche das Risiko quantitativ beschreiben und dadurch Risikoinformationen insbesondere für die Unternehmenssteuerung zur Verfügung stellen [Romeike & Hager 2009, S. 146].

Im Zuge einer **ausführlichen Dokumentation** werden die wesentlichen Informationen zu den im Risiko- & Compliancemanagement adressierten Risiken in einem sogenannten Risiko-Steuerungsinventar gesammelt, das zumindest folgende Punkte beinhalten sollte:

- Identifizierte Risiken,
- Qualitative oder Quantitative Bewertungen der Risiken,
- Steuerungsmaßnahmen zur Bewältigung der Risiken,
- Verantwortlichkeiten für die Steuerungsmaßnahmen,
- Beurteilung der Wirksamkeit der bestehenden Steuerungsmaßnahmen.

Somit kann folgendes Unterkriterium für das Risiko- & Compliancemanagement auf Reifegrad 3 definiert werden:

R-&CM-Kriterium für Reifegrad 3
Der Einsatz von **Risikomaßen** ermöglicht einen Vergleich verschiedener Risiken mit unterschiedlichen Charakteristika, Verteilungsformen und -parametern. **Risikoindikatoren** dienen in Verbindung mit einem Ampelsystem als Frühwarnsystem. Ein **Risiko-Steuerungsinventar** beinhaltet alle identifizierten Risiken und deren qualitative und quantitative Bewertung. Des Weiteren werden entsprechende Steuerungsmaßnahmen zur Risikobewältigung, Verantwortlichkeiten sowie die Beurteilung der Wirksamkeit der bestehenden Steuerungsmaßnahmen darin festgehalten.

5.3.3 Integrativer Ansatz im R-&CM

Analog zum integrativen Ansatz im risikobasierten Prozessmanagement.

5.4 Reifegrade der Internen Revision

Wie in den vorigen Kapiteln angeführt, werden die in der Internen Revision adressierten Risiken im Zuge dieser Arbeit als Konformitätsrisiken bezeichnet (Abbildung 29).

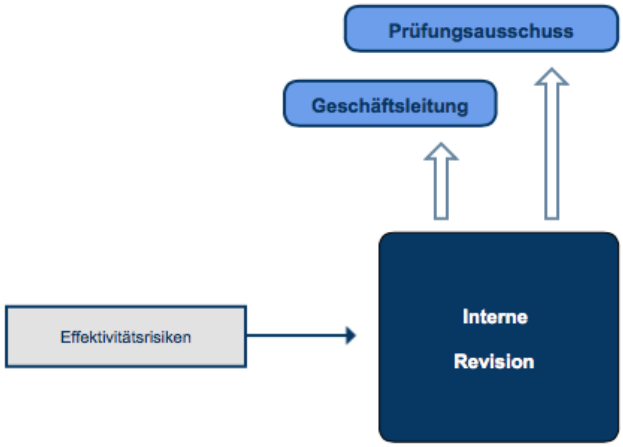


Abbildung 29: Risiken in der Internen Revision

5.4.1 Strukturierte Risikobeurteilung und -bewältigung in der IR

Die Interne Revision ist, wie in Kapitel 4.4 erläutert, im Allgemeinen im Unternehmen dafür verantwortlich, dass entsprechende Kontroll- und Steuerungsmaßnahmen seitens des risikobasierten Prozessmanagements und des Risiko- & Compliancemanagements eingehalten werden. Somit können die Prüfungs- und Beratungsdienstleistungen der Internen Revision, falls vorhanden, sowohl als strukturierte Risikobeurteilung als auch als strukturierte Risikobewältigung interpretiert werden, mit denen Gefahren des Nichteinhaltens bestimmter Vorgaben (Konformitätsrisiken) abgewendet werden können.

IR-Kriterium für Reifegrad 2
Die Interne Revision prüft mit entsprechenden Prüfdienstleistungen, ob die vorgesehenen Kontrollmaßnahmen des risikobasierten Prozessmanagements und Steuerungsmaßnahmen des Risiko- & Compliancemanagements auch eingehalten werden.

5.4.2 Quantitative Leistungssteuerung und ausführliche Dokumentation in der IR

Im Zuge der **quantitativen Leistungssteuerung** spielen in der internen Revision, ähnlich wie beim risikobasierten Prozessmanagement, vorwiegend Risikoindikatoren eine bedeutende Rolle.

Im Sinne einer **ausführlichen Dokumentation** der Internen Revision sollte ein Risiko-Prüfinventar folgenden Mindeststand aufweisen:

- Ablauf der Prüf- und Beratungsdienstleistungen,
- Zeitpunkt der Prüf- und Beratungsdienstleistungen,
- Verantwortlichkeiten der Prüf- und Beratungsdienstleistungen.

IR-Kriterium für Reifegrad 3
Risikoindikatoren werden zur Überprüfung der Wirksamkeit der Prüfungs- und Beratungsdienstleistungen herangezogen. Ein Risiko-Prüfinventar beinhaltet den Ablauf aller Prüf- und Beratungsdienstleistungen, Zeit der Erbringung dieser Dienstleistung sowie Ergebnisse und den dafür Verantwortlichen.

5.4.3 Integrativer Ansatz in der IR

Neben der Durchführung unabhängiger interner Prüfungsmandate ist bei der Internen Revision die Berichterstattung an die Geschäftsführung und den Prüfungsausschuss von zentraler Bedeutung. Im Sinne eines integrierten Management-Systems werden entsprechende Daten seitens der Internen Revision der Geschäftsführung bereitgestellt. Dadurch unterstützt die Interne Revision die Geschäftsführung in ihrer Kontroll-, Steuerungs- und Lenkungsfunktion.

IR-Kriterium für Reifegrad 4
Die Interne Revision berichtet der Geschäftsführung und dem Prüfungsausschuss im vollem Umfang über die Ergebnisse der Prüfdienstleistungen und unterstützt die Geschäftsführung in deren Kontroll-, Steuerungs- und Lenkungsfunktion.

5.5 Reifegradmodell für das unternehmensweite RM

Abbildung 30 zeigt alle in den vorigen Kapiteln abgeleiteten Reifegrad-Kriterien der einzelnen RM-Funktionen zusammengefasst.

	Risikoorientiertes Prozessmanagement	Risiko- & Compliancemanagement	Interne Revision
RG 1: Initial	• Keine Modellierung der wichtigsten Geschäftsprozesse.	• Das Unternehmen ist sich ihrer wesentlichen Erfolgspotenziale nicht bewusst. • Kein Compliance-Verständnis.	• Es finden keine Prüfdienstleistungen zur Überprüfung des risikobasierten Prozessmanagements und Risiko- & Compliancemanagements statt.
RG 2: Geführt	• Basierend auf der Modellierung der wesentlichen Geschäftsprozesse werden durch die jeweiligen Anforderungen an Leistung, Qualität, finanzielle Berichterstattung und Compliance entsprechende Risiken abgeleitet und bewertet. • Zur Vermeidung bzw. Verringerung dieser Risiken werden geeignete manuelle oder automatische Kontrollmaßnahmen bestimmt.	• Aus den **Bedrohungen** der für das Unternehmen wichtigen **Erfolgspotenziale** werden **strategische** und **finanzielle Risiken** identifiziert und bewertet. • Die für das Unternehmen **relevanten Rechtsgebiete** sind bekannt und werden zur Identifizierung bzw. Bewertung der **Compliance-Risiken** herangezogen. • Um Risiken zu Vermeiden, Verringern, Teilen oder Akzeptieren werden entsprechende **Steuerungsmaßnahmen** bestimmt.	• Die Interne Revision prüft mit entsprechenden Prüfdienstleistungen, ob die vorgesehenen Kontrollmaßnahmen des risikobasierten Prozessmanagements und Steuerungsmaßnahmen des Risiko- & Compliancemanagements auch eingehalten werden.
RG 3: Quantitativ geführt	• Risikoindikatoren dienen in Verbindung mit einem Ampelsystem als Frühwarnsystem. • Unter Verwendung gängiger Modellierungssprachen werden die wesentlichen Geschäftsprozesse präzise modelliert. • Ein ausführliches Risiko-Kontrollinventar beinhaltet alle identifizierten Risiken und die entsprechenden Kontrollmaßnahmen zu deren Bewältigung sowie die dafür vorgesehenen Verantwortlichen.	• Der Einsatz von **Risikomaßen** ermöglicht einen Vergleich verschiedener Risiken mit unterschiedlichen Charakteristika, Verteilungsformen und -parametern. • **Risikoindikatoren** dienen in Verbindung mit einem Ampelsystem als Frühwarnsystem. • Ein **Risiko-Steuerungsinventar** beinhaltet alle identifizierten Risiken und deren qualitative und quantitative Bewertung. Des Weiteren werden entsprechende Steuerungsmaßnahmen zur Risikobewältigung, Verantwortlichkeiten sowie die Beurteilung der Wirksamkeit der bestehenden Steuerungsmaßnahmen darin festgehalten.	• Risikoindikatoren werden zur Überprüfung der Wirksamkeit der Prüfungs- und Beratungsdienstleistungen herangezogen. • Ein Risiko-Prüfinventar beinhaltet den Ablauf aller Prüf- und Beratungsdienstleistungen, Zeit der Erbringung dieser Dienstleistung sowie Ergebnisse und den dafür Verantwortlichen.
RG 4: Optimiert	• Durch die gemeinsame Nutzung einer IT-gestützten Plattform können das risikobasierte Prozessmanagement und das Risiko- & Compliancemanagement gleiche Daten über Prozesse, Kennzahlen und relevante Risikoinformationen abgleichen bzw. austauschen und so Diskrepanzen und Doppelgleisigkeiten vermieden werden.		• Die Interne Revision berichtet der Geschäftsführung und dem Prüfungsausschuss im vollem Umfang über die Ergebnisse der Prüfdienstleistungen.

Abbildung 30: Reifegradmodell für das unternehmensweite RM

5.6 Fragebogen-Entwurf zur Bewertung des unternehmensweiten RM

Der nachfolgende Fragebogen soll einen ersten Vorschlag darstellen, um die Kriterien der einzelnen Reifegrade aus dem Modell (Abbildung 30) zu verifizieren:

Fragen für das risikobasierte Prozessmanagement	
Wie werden Prozessleistungsrisiken im Unternehmen beurteilt?	**RG 2**
Wie werden Qualitätsrisiken im Unternehmen beurteilt?	**RG 2**
Wie werden Berichterstattungsrisiken im Unternehmen beurteilt?	**RG 2**
Welche Kontrollmaßnahmen werden zur Bewältigung von Prozessleistungsrisiken eingesetzt?	**RG 2**
Welche Kontrollmaßnahmen werden zur Bewältigung von Qualitätsrisiken eingesetzt?	**RG 2**
Welche Kontrollmaßnahmen werden zur Bewältigung von Berichterstattungsrisiken eingesetzt?	**RG 2**
Welche Risikoindikatoren dienen im Unternehmen als Frühwarnsystem?	**RG 3**
Welche Modellierungssprachen werden zur Abbildung der wesentlichen Geschäftsprozesse verwendet?	**RG 3**
Welche Informationen beinhaltet das Risiko-Kontrollinventar?	**RG 3**
Wie werden Daten über Prozesse und relevante Risikoinformationen mit dem Risiko- & Compliancemanagement abgeglichen bzw. ausgetauscht?	**RG 4**

Fragen für das Risiko- & Compliancemanagement	
Wie werden strategische Risiken beurteilt?	**RG 2**
Wie werden finanzielle Risiken beurteilt?	**RG 2**
Wie werden Compliance-Risiken im Unternehmen beurteilt?	**RG 2**
Welche Steuerungsmaßnahmen werden zur Bewältigung von strategischen Risiken eingesetzt?	**RG 2**
Welche Steuerungsmaßnahmen werden zur Bewältigung von finanziellen Risiken eingesetzt?	**RG 2**

Welche Steuerungsmaßnahmen werden zur Bewältigung von Compliance-Risiken eingesetzt?	**RG 2**
Welche Risikomaße finden im Unternehmen Anwendung?	**RG 3**
Welche Risikoindikatoren dienen im Unternehmen als Frühwarnsystem?	**RG 3**
Welche Informationen beinhaltet das Risiko-Steuerungsinventar?	**RG 3**
Wie werden Daten über Prozesse und relevante Risikoinformationen mit dem Risiko- & Compliancemanagement abgeglichen bzw. ausgetauscht?	**RG 4**

Fragen für die Interne Revision	
Welche Prüf- und Beratungsdienstleistungen werden seitens der Internen Revision erfüllt?	**RG 2**
Welche Risikoindikatoren werden zur Überprüfung der Wirksamkeit der Prüfdienstleistungen herangezogen?	**RG 3**
Welche Informationen beinhaltet das Risiko-Prüfinventar?	**RG 3**
Welche Informationen werden seitens der Internen Revision an die Geschäftsführung und den Prüfungsausschuss berichtet?	**RG 4**

Kapitel 6

Zusammenfassung und Ausblick

Zusammenfassung

Zentraler Punkt in Kapitel 1 war die Diskussion der Notwendigkeit einer unternehmensweiten Betrachtung des Risikomanagements im Sinne von COSO II bei der Entwicklung bzw. beim Einsatz von Reifegradmodellen.

In Kapitel 2 wurde die für diese Arbeit wichtigen theoretischen Grundlagen von Reifegradmodellen eingegangen und im Speziellen das von der Carnegie Mellon University entwickelte Capability Maturty Model Integration (CMMI) vorgestellt.

Kapitel 3 beschäftigt sich zu Beginn mit dem Risikobegriff und stellt anschließend die zur Entwicklung des Reifegradmodells notwendigen theoretischen Grundlagen aus dem Risikomanagement bereit. Dabei wird auf die Schwerpunkte des COSO II Rahmenwerks, der ISO 31000 und des Three Lines of Defense Models eingegangen und deren wesentlichen Kernelemente erläutert.

Im Zuge von Kapitel 4 wird das 3LoD-Modell als Referenzmodell herangezogen, um die RM-Funktionen innerhalb des Unternehmen voneinander abzugrenzen und vorhandene Synergien aufzuzeigen.

Basierend auf den Reifegraden des CMMI werden abschließend in Kapitel 5 geeignete ERM-Reifegrad-Kriterien hergeleitet, auf die einzelnen RM-Funktionen konkretisiert und in einem Reifegradmodell für das unternehmensweite Risikomanagement zusammengefasst.

Beiträge der Arbeit

Basierend auf den CMMI-Reifegraden wurden die ISO 31000-Inhalte einzelnen ISO 31000-Reifegrad-Kriterien zugeordnet. Dadurch wurde die notwendige CMMI-Konformität für das Risikomanagement-Reifegradmodell sichergestellt. Die Vorteile, welche sich aus der Weiterentwicklung des CMM zum CMMI ergaben, konnten somit in das Risikomanagement-Reifegradmodell miteinfließen.

Durch das 3LoD-Modell wurden die einzelnen RM-Funktionen im Unternehmen abgegrenzt und eindeutige Synergiepotenziale aufgezeigt. Aus der Bedrohung der einzelnen Ziele der RM-Funktionen konnten die unterschiedlichen Risiken abgeleitet werden und den einzelnen Säulen des 3LoD-Modells zugeteilt werden. Somit ermöglichte das Einbeziehen der unternehmensweiten Definition des Risikomanagements nach dem COSO II-Verständnis eine klare Risikokategorisierung aller im Unternehmen anfallenden Risiken.

Die aus den ISO 31000-Reifegrad-Kriterien abgeleiteten ERM-Reifegrad-Kriterien konnten auf die unternehmensweiten RM-Funktionen konkretisiert werden. Dadurch ergaben sich die jeweiligen Kriterien der Reifegrade für die einzelnen Säulen im 3LoD-Modell. Diese Kriterien wurden anschließend zum Reifegradmodell für das unternehmensweite Risikomanagement zusammengefasst.

Nutzenmöglichkeiten

Ein erster Nutzen ergibt sich aus der abgeleiteten Risikokategorisierung. Unternehmen können sich damit einen Überblick aller wesentlichen Risiken im Unternehmen machen. Des Weiteren ist durch die Zuteilung der Risiken im 3LoD-Modell eindeutig ersichtlich, wo im Unternehmen welche Risiken adressiert werden. Dabei ist das risikobasierte Prozessmanagement vorwiegend für die Risikobewältigung im Zuge des Tagesgeschäfts verantwortlich, wohingegen finanzielle und strategische Risiken auf sehr hohem Niveau ausschließlich im Risiko- & Compliancemanagement adressiert werden.

Ein entscheidender Vorteil dieser Darstellung ergibt sich aus der Tatsache, dass der jeweilige, oft unterschiedliche, Ausbaugrad der einzelnen RM-Funktionen nicht von Bedeutung ist. So ist es nicht ausschlaggebend, ob die erste Säule, also das risikobasierte Prozessmanagement, aus dem Prozessmanagement, Qualitätsmanagement oder Internem Kontrollsystem aufgebaut ist. Nicht das „wo“, sondern das „ob“ ist bei der Beurteilung des Reifegrades von Bedeutung. Demnach kann ein Unternehmen ohne Prozessmanagement, jedoch mit einem entsprechend ausgebauten Qualitätsmanagement oder Internen Kontrollsystem, ebenfalls Reifegrad 4 erreichen. Haben Unternehmen ein Internes Kontrollsystem nach COSO I implementiert, könnte dieses, wenn entsprechend ausgebaut, ebenfalls sämtlichen Risiken der ersten Säule erfolgreich begegnen.

Der wohl größte Vorteil des unternehmensweiten Risikomanagement-Reifegradmodells ist das Miteinbeziehen aller im Unternehmen vorhandenen RM-Funktionen. Dadurch ergibt sich die Möglichkeit einer gezielten Fehlerquellenanalyse. So kann das Ergebnis der Reifegradbeurteilung eine klare Auskunft darüber geben, wo im Unternehmen Verbesserungspotenzial besteht. Dabei zeigt ein entsprechend geringer Reifegrad des risikobasierten Prozessmanagements auf, dass der operative Teil, also das Risikomanagement, Handlungsbedarf im Zuge des Tagesgeschäfts benötigt. Dafür können schlecht modellierte Geschäftsprozesse genauso verantwortlich sein, wie das Fehlen manueller bzw. automatischer Kontrollmaßnahmen. Auf der anderen Seite impliziert ein niedriger Reifegrad des Risiko- & Compliancemanagements die Notwendigkeit von Steuerungsmaßnahmen zum Vermeiden, Verringern, Teilen bzw. gezielten Akzeptieren finanzieller, strategische und Compliance-Risiken.

Zukünftige Herausforderungen

Eine wesentliche zukünftige Herausforderung stellt der Ausbau bzw. die Weiterentwicklung des Fragebogens dar. Der im Zuge dieser Arbeit entstandene Entwurf stellt lediglich einen Vorschlag bereit, der weder den Anspruch auf Vollständigkeit noch auf Validierung der Kriterien haben soll.

Ziel sollte somit die Entwicklung eines entsprechenden Fragebogens sein, welcher für empirische Analysen verwendet werden kann. Dieser würde zum Beispiel eine Analyse österreichischer Unternehmen bezüglich ihres unternehmensweitem Risikomanagement erlauben. Eine anschließende Interpretation ließe dann auf den aktuellen Stand des unternehmensweiten Risikomanagements österreichischer Unternehmen schließen.

Literaturverzeichnis

AUSTRIA, Institut für Interne Revision Österreich - IIA (ed). 2009. *Das Interne Kontrollsystem aus der Sicht der Internen Revision*. Wien: Linde-Verlag.

AUSTRIA, Institut für Interne Revision Österreich - IIA (ed). 2014. *Das unternehmensweite Risikomanagementsystem aus der Sicht der Internen Revision*. Wien: Linde-Verlag.

BECKER, Jörg, Ralf KNACKSTEDT, and Jens PÖPPELBUß. 2009. Entwicklung von Reifegradmodellen für das IT-Management – Vorgehensmodell und praktische Anwendung. *Wirtschaftsinformatik*.

BERLE, Adolph and Gardiner MEANS. 1932. *The Modern Corporation and Private Property*. New York: Macmillan-Verlag.

BRÜHEIM, Andreas and Tobias SCHMIEMANN. 2013. *Risk-Controlling und Wertorientiertes Management*. Marburg: Tectum-Verlag.

BRÜHWILER, Bruno. 2007. *Risikomanagement als Führungsaufgabe*. Stuttgart: Haupt-Verlag.

BRÜHWILER, Bruno. 2008. Neue Standards im Risikomanagement. *MQ - Magangement und Qualität*.

BRÜHWILER, Bruno and Frank ROMEIKE. 2010. *Praxisleitfaden Risikomanagement - ISO 31000 und ONR 49000 sicher anwenden*. Berlin: Erich Schmidt-Verlag.

BRUNNER, Andreas and Josef LUTHIGER. 2009. Corporate Risk Management - KMU nachhaltig sichern durch operatives Risikomanagement. *KMU-Magazin*. **Nr. 4**.

BUNGARTZ, Oliver. 2011. *Handbuch Interne Kontrollsysteme (IKS)*. Berlin: Erich Schmidt-Verlag.

CADBURY, Adrian. 1992. *Report of the Committee on financial Aspects of the Corporate Governance*. London: The Committee on the Financial Aspects of Corporate Governance and Gee and Co. Ltd.

CHRISSIS, Mary Beth, Mike KONRAD, and Sandy SHRUM. 2006. *CMMI®: Richtlinien für Prozess-Integration und Produkt-Verbesserung*. München: Addison Wesley-Verlag.

COTTIN, Claudia and Sebastian DÖHLER. 2013. *Risikoanalyse - Modellierung, Beurteilung und Management von Risiken mit Praxisbeispielen*. Wiebaden: Springer Spektrum-Verlag.

CROSBIE, Peter. DECEMBER 18, 2003. *„Modeling default risk" , Modeling Methodology*. Moody's KMV.

CROSBY, Philip B. 2000. *Qaulitätsmanagement - Die aktuellste Auflage des Bestsellers "Quality is free"*. Wien: Ueberreuter-Wirtschaftsverlag.

DE BRUIN, Tonia, Michael ROSEMANN, Ronald FREEZE, and Uday KAULKARNI. 2005. nderstanding the main phases of developing a maturity assessment model. *In*: *16th Australasian conference on infor- mation systems*. Sydney.

DIEDERICHS, Marc. 2010. *Risikomanagement und Risikocontrolling. Risikocontrolling - ein integrierter Bestandteil einer modernen Risikomanagement-Konzeption*. München: Vahlen-Verlag.

EKKENGA, Jörg and Andreas KRAMER. 2011. Umsetzung und Praxis. *In*: *Risikomanagement und Risiko-Controlling*, Wien: Haufe Verlag, pp.113-135.

ERBEN, Roland Franz. 2011. Risikokonvergenz. *Manager Magazin*.

ERTL, Peter. 2009. Dimensionen. *Schwerpunkt Wirtschaftskrise*, Jänner.

ERT-WAGNER, Birgit, Sabine STEINBRUCKER, and Bernd C. WAGNER. 2009. *Qualitätsmanagement und Zertifizierung - Praktische Umsetzunng in Krankenhäusern, Reha-Kliniken, stationären Pflegeeinrichtungen*. Heidelberg: Springer Medizin Verlag.

FRASER, Peter, James MOULTRIE, and Mike GREGORY. 2002. The use of maturity models/grids as a tool in assessing product development capability. *IEEE Engineering Management Society*.

GAUSEMEIER, Jürgen and Christoph PLASS. 2014. *Zukunftsorientierte Unternehmensgestaltung - Strategien, Geschäftsprozesse und IT-Systeme für die Produktion von morgen*. München: Carl Hanser-Verlag.

GLEISSNER, Werner. 2004. Die Aggregation von Risiken im Kontext der Unternehmensplanung. *ZfCM - Zeitschrift für Controlling & Management*, pp.350-359.

GLEISSNER, Werner. 2011. *Grundlagen des Risikomanagements im Unternehmen*. München: Vahlen-Verlag.

GLEISSNER, Werner. 2011. Quantitive Verfahren im Risikomanagement: Risikoaggregation, Risikomaße und Performancemaße. *Der Controlling-Berater*. 16, pp.179-204.

GREINER, Saskia. 2013. Risikoorientierte Prozessmodelle in BPMN – Stand des Wissens und Potenziale. *In*: *IT-gestütztes Ressourcen- und Energiemanagement* , Berlin: Springer Verlag, pp.209-218.

HILLSON, David. 1197. Towards a Risk Maturity Model. *The Internatinal Journal of Project & Business Risk Management*. Nr. 1, pp.35-45.

HOFFMANN, Jürgen. 2012. *Risikomanagement für mittelständige Unternehmen*. Norderstedt: Books on Demand-Verlag.

HOFMANN, Ines. 2013. *Risikomanagement und Controlling*. Wien: Verlag des Österreichischen Gewerkschaftsbundes GmbH.

HUNZIGER, Stefan. 2011. *Internes Kontrollsystem: Synergien mit dem Risikomanagement und anderen Managementsystemen - einige Aspekte*. Zürich: Weka Verlag.

HUNZIGER, Stefan, Hermann GRAB, Yvonne DIETIKER, and Lothar GWERDER. 2012. *IKS Leitfaden - Internes Kontrollsystem für Gemeinden*. Bern: Haupt-Verlag.

IIA Positions Paper: The three Lines of Defense in effective Risk Management and Control. 2013.

Integrierte Managementsysteme (IMS) Handlungsanleitung zur praxisorientierten Einführung Beispiele aus der Praxis (VDI 4060, Blatt 2). 2005. Berlin: Beuth Verlag.

KÜBEL, Moritz. 2013. *Corporate M&A - Reifegradmodell und empirische Untersuchung*. Wiebaden: Springer Gabler-Verlag.

KÖNIG, Hans-Peter. 2013. *IT-Risikomanagement mit System - Praxisorientiertes Management von Informationssicherheits- und IT-Risiken*. Wiesbaden: Springer-Verlag.

KAMPRATH, Nora. 2011. Einsatz von Reifegradmodellen im Prozessmanagement. *HMD - Praxis der Wirtschaftsinformatik*.

KAPLAN, Robert S. and Anette MIKES. 2012. Managing Risks: A New Framwork. *Harvard Business Review*.

KEMPE, Thomas. 2004. *Management wetterinduzierter Risiken in der Energiewirtschaft*. Wiesbaden: Deutscher Universitäts-Verlag.

KLINGER, Michael A. and Oskar KLINGER. 2009. *Das Interne Kontrollsystem im Unternehmen: Checklisten, Organisationsanweisungen, Praxisbeispiele und Muster-Prüfberichte*. München: Vahlen Verlag.

KROPP, Matthias and Robert M. GILLENKIRCH. 2004. Controlling von Finanzrisiken in Industrieunternehmen. *Zeitschrift für Controlling und Management*, pp.86-96.

KRUSE, Wenke. 2009. *Prozessoptimierung am Beispiel der Einführung eines neuen selbstverantwortlichen Arbeitsplanungsmodells im Hanse-Klinikum Wismar*. Bremen: Europäischer Hochschulverlag.

KUHLANG, Peter. 2013. *Prozessmanagement*. Wien.

LÜCK, Wolfgang and Anja UNMUTH. 2006. Interne Revision und Risikomanagement. *In*: *Zentrale Tätigkeitsbereiche der Internen Revision*, Berlin: Erich Schmidt-Verlag, pp.11-33.

LÖHR, Benjamin W. 2010. *Integriertes Risikocontrolling für Industrieunternehmen - Eine normative Konzeption im Kontext der Controllingforschung von 1990 bis 2009*. Frankfurt am Main: Internationaler Verlag der Wissenschaften.

MÜLLNER, Thomas, Tim FARCHER, and Robert STROBL. 2013. Integration von Prozess- und Risikomanagement durch das Interne Kontrollsystem. *In*: Franz BAYER and Harald KÜHN, (eds). *Prozessmanagement für Experten - impulse für aktuelle und wiederkehrende Themen*, Berlin: Springer Gabler Verlag, pp.333-354.

MADREITER, Michael S. 2013. Business Pulse: Toprisiken und -chancen in 2013 und darüber hinaus. *Finance Newsletter*, Mai.

MARX, Frederik, Felix WORTMANN, and Jörg H. MAYER. 2012. *Wirtschaftsinformatik*.

MERZ, Mirjam. 2011. *Entwicklung einer indikatorenbasierten Methodik zur Vulnerabilitätsanalyse für die Bewertung von Risiken in der industriellen Produktion*. Karlsruhe: KIT Scientific Publishing.

METTLER, Tobias. 2010. *Supply Management im Krankenhaus - Konstruktion und Evaluation eines konfigurierbaren Reifegradmodells zur zielgerichteten Gestaltung*. Göttingen: Sierke-Verlag.

MOTT, Bernd P. 2001. Organisatorische Gestaltung von RisikoManagement-Systemen. *In*: *Wertorientiertes Risikomanagement für Industrie und Handel* , Wiesbaden: Gbeler-Verlag, pp.199-232.

OCHSNER, Peter. 2013. Corporate Governance - Ein Führungssystem mit Checks & Balances. *Disclose - Im Fokus: Corporate Governance*, Juni, pp.5-7.

PIELERT, Michael. 2013. *Internes Rating als Monitoringtool des Finanzwesens*. Kassel: Kassel University Press.

PRICE WATERHOUSE COOPERS. 2007. *www.pwc.ch*. [online]. [Accessed 20 März 2014]. Available from World Wide Web: <http://www.pwc.ch/user_content/editor/files/publ_ass/pwc_iks_fuehrungsinstrument_wandel_06_d.pdf>

RÖGLINGER, Maximilan and Nora KAMPRATH. 2012. Prozessverbesserung mit Reifegradmodellen - Eine Analyse ökonomischer Zusammenhänge. *Zeitschrift für Betriebswirtschaft*, April.

RAUTENSTRAUCH, Thomas and Stefan HUNZIGER. 2011. *Ist Ihr Risikomanagement effektiv und effizient? - Drei Tests zur Überprüfung der Leistungsfähigkeit*. Zürich: WEKA-Verlag.

RIEKE, Tobias and Axel WINKELMANN. 2008. Modellierung und Management von Risiken – Ein prozessorientierter Risikomanagement-Ansatz zur Identifikation und Behandlung von Risiken in Geschäftsprozessen. *Wirtschaftsinformatik 50 , S. 346 - 356.* **5**, pp.146-156.

ROMEIKE, Frank. 2003. Der Prozess des strategischen und operativen Risikomanagements. *In*: *Erfolgsfaktor Risiko-Management*, Wiebaden: Gabler-Verlag.

ROMEIKE, Frank. 2003. Gesetzliche Grundlagen, Einordnung und Trends. *In*: *Erfolgsfaktor Risiko-Management*, Wiesbaden: Gabler-Verlag.

ROMEIKE, Frank and Gerrit Jan BRINK. 2006. Frühwarnindikatoren: Kritischer Faktor Spätwarnung. *Risiko Manager*.

ROMEIKE, Frank and Peter HAGER. 2009. *Erfolgsfaktor Risiko-Management 2.0 - Methoden, Beispiele, Checklisten*. Wiebaden: Gabler Verlag.

ROMMELFANGER, Heinrich. 2008. *Risikoaggregation in der Praxis - Beispiele und Verfahren aus dem Risikomanagement von Unternehmen*. Berlin: Springer-Verlag.

SCHERPEREEL, Peter. 2006. *Risikokapitalallokation in dezentral organisierten Unternehmen*. Wiesbaden: Deutscher universitäts-Verlag.

SCHNECK, Ottmar. 2010. *Risikomanagement: Grundlagen, Instrumente, Fallbeispiele*. Weinheim: Wiley-VCH-Verlag.

SCHNEIDER, Gabriel, Ingrid Katharina GEIGER, and Johannes SCHURING. 2008. *Prozess- und Qualitätsmanagement - Grundlagen der Prozessgestaltung und Qualitätsverbesserung mit zahlreichen Beispielen, Repetitionsfragen und Antworten*. Zürich: Compendio Bildungsmedien AG.

SCHWAIGER, Walter S.A. 2012. *Controlling: Planung, Kontrolle und Lenkung im Zeitablauf*. Wien.

SHLEIFER, Andre and Robert W. VISHNY. 1986. Large shareholder and Corporate Control. *Journal of Political Economy 94*. Nr. 3, pp.461-488.

SOMMER, Materine. 2010. *Risikoorientiertes Zusammenwirken der Internal Control, des Risikomanagements, des Internen Audits und der Externen Revision*. St.Gallen: Difo-Druck GmbH.

STEPHAN, Jörg. 2006. *Finanzielle Kennzahlen for Industrie- und Handelsunternehmen - Einewert- und risikoorientierte Perspektive*. wiebaden: Deutscher Universitäts-Verlag.

THEUERMANN, Chrisitan and Gerhart EBNER. 2012. *Risikomanagement im österreichischen Mittelstand - Verbreitung, Bedeutung und zukünfitige Erwartungen*. Graz.

TRAMBO, Uwe, Martina MÜLLER, Verena REGELE, and Thomas SONTHEIM. 2010. *Identifikation und Analyse von Prozessrisiken*.

UNIVERSITY, Carnegie Mellon. 2010. *CMMI für Entwicklung - Version 1.3*. Pittsburgh.

WAGNER, Karl W. and Roman KÄFER. 2013. *PQM - Prozessorientiertes Qualitätsmanagement*. München: Hanser Verlag.

WENGERT, Holger and Frank Andreas SCHITTENHELM. 2013. *Corporate Risk Management*. Heidelberg: Springer-Verlag.

WIENDAHL, Hans-Peter. 2014. *Betriebsorganisation für Ingenieure*. München: Hanser Verlag.

WIGGERT, Marcel M. 2009. Risikomanagement von Betreiber- und Konzessionsmodellen. *Schriftenrehe der TU Graz*.

WINTER, Peter. 2007. *Risikocontrolling in Nicht-Finanzunternehmen: Entwicklung einer tragfähigen Risikocontrolling-Konzeption und Vorschlag zur Gestaltung einer Risikorechnung*. Köln: Eul-Verlag.

ZUBER, Pascal. 2008. *Innovationsmanagement in der Biotechnoligie - Nachhaltigkeit als Leitbild einer entwicklungsbegleitenden Evulation*. Wiesbaden: Gabler-Verlag.